An Introduction to New Technologies

PART 1

By Patrick Redmond

Patrick Redmond graduated with a Doctorate in History from the University of London, England in 1972. He taught at the University of the West Indies in Trinidad, then at Adhadu Bello University in Kano, Nigeria before joining IBM. He worked in IBM for 31 years before retiring. During his career at IBM he held a variety of jobs. These included; from 1992 until 2007 working at the IBM Toronto lab in technical, then in sales support. He has written two books and numerous articles. Here is a presentation he gave in Toronto on April 13, 2008.

* * *

I want to thank Yvon for inviting me here to talk about new technologies. What I'm going to do is give you an introduction to three technologies that are becoming more and more important. The first is RFID chips, the second genetic engineering, and the third synthetic biology. This will give you an understanding of what is happening and where science is going.

We will start with RFID chips:

So what are they? They are Radio Frequency Identification Devices. An RFID is a microchip with an attached antenna. The microchip contains stored information which can be transmitted to a reader and then to a computer.

RFID's can be passive, semi-passive or active. Active RFID's have an internal power source such as a battery. This allows the tag to send signals back to the reader, so if I have a RFID on me and it has a battery, I can just send a signal to a reader wherever it is. They can receive and store data, and be read at a further distance than the passive RFID's. The batteries can only last a short while. But the current batteries in the RFID's can last for over a hundred years, because of their self-generating power. Ultra-wideband (UWB) allows the small battery operated RFID tag to be sensed over fairly wide areas. For instance, GE Aircraft Engines in Ohio has installed five readers in the factory and it covers over 30,000 square feet so they can track everything within that area with only the five readers. That gives you an idea of the distance that can be covered by an RFID tag that might be on you or on equipment.

The readers can transmit over telephone or by internet to computers and they use satellites as well. For example, Digital Angel has signed contracts with satellite providers to transmit their data for military personnel location beacons (PLBs). These beacons use the COSPAS-SARSAT satellite system. This system has some 400,000 digital beacons around the world and it's rising to some 900,000. By the year 2009 they plan to have a GL stationary satellite system that will enable them to find the location and details of any beacon. You may sometimes see these at night; the GO stationary systemscan track any beacon. Skiers sometimes use them so that they can be identified, and sailors as well, if they become lost at sea they will be able to be tracked. Anything that has an RFID tag can be tracked by a reader or a computer.

An example of such transmission is a chip sold by Zarlink. This chip is implanted in a person; it tracks problems and if one is detected, it alerts the doctor who uses a two way RF link to interrogate and adjust the implanted device. Semi-passive RFIDs have an internal power source that let them monitor environmental conditions, such as temperature and shock, but they still require RF energy from the reader to respond.

Passive RFID's do not have a power source but use a signal sent by the scanner to power the microchip circuit to transmit back their stored information. Passive RFID's are getting very small. Hitachi a few years ago produced a chip (called the mu chip) that was the size of a pencil point; if you take a pencil and put it on a piece of paper you get a little dot. That's how small they're getting. In 2007 Hitachi came out with a chip that was even smaller, they call it RFID powder. They are just like the talcum powder you would put on a baby.

Somark Innovations in Jan 10, 2007 announced an invisible RFID ink. This can be applied to cattle, prime cuts of meat, military personnel and it can be read through hair.

I brought along a couple of the larger size chips, and this particular chip I got from Gillette fusion blades. I bought one of the blades and you can see that on one side what looks like a bar code and if you open it up you can see parts of a RFID chip on the back. This one here is from the Gap. One of my daughters went to the Gap; they put the tag directly on the clothing and the instructions just say to remove before washing and wearing. If you put it up to the light you will see the RFID chip inside it. These chips are quite small and can be put on the back of labels. They would not be noticeable in badges or ID cards; they could even be put in the eye of a person, they are that small.

In order for chips to be useful, they have to have a unique product number and because of this, MIT (Massachusetts Institute of Technology) started developing some standards. It's called the AutoID Center. They then passed it on to the AutoID Group within the Uniform Clothes Council. It will assign codes and publish specifications, so if you have a company, government agency, or church you can contact these people and they will give you a set of numbers.

So let's say there are three or five people in this room wearing the same white hat and each one of them has a chip on it with a different number. We could differentiate everything even if you're all wearing the same clothes, it doesn't really matter because everything has a unique number. MIT has the architecture of participation called EPC Global so if you go on Google and type in EPC Global and you will come up with the website they will give you instructions on how to apply and get chips. So if you want to chip yourself, your family, relatives, company or anything like that; you can do it.

It works with people who want to use this technology. One of many companies who sell the chip is called, Technic Imitations. If you have a company and you go to one of their presentations, they will give you books like this that tell you what the chips look like, how they work, the types that are sold, and what the readers look like. They will help you install chips in your company. It's a very big business and it's spreading very quickly.

When you use active or passive chips, active chips have advantages when you want to track items or people over longer distances. Soldiers can have active chips so they can be tracked via satellite wherever they might be in the battlefield. You can get one for your car, so you can be tracked if you are on the 407 or something.

Passive ones suffice if you are only interested in tracking over shorter distances. For example, in a sea container coming in from China, every box and every item within the box can have a chip on it. A reader can track all the items as a box passes through it. In a warehouse it is used to ensure the right shipments go to the right places. A man carrying a skid on a forklift can have the goods inside the box verified without even opening it.

They are using the chips to track inventory in order to be able to monitor what items are going where, if the right items are in the truck, etc. The passive chips are being put on devices to ensure they are valid.

There's a lot of counterfeit drugs being produced and sold over the internet. Viagra is one of the most commonly counterfeited ones although there are many others. To ensure that people get the correct drugs they sometimes put chips on the containers so when you're buying them you know that you are buying the correct drug.

RFID's are a great economic help to a company because they reduce theft and loss. They also streamline inventory, reduce turnaround time and handling. They've allowed companies to adjust production in response to inventory levels and to respond on demand. That's why companies are interested, because of these big economic benefits and efficiency.

When you go to Wal-Mart, Best Buy, the U.S. Military and many other agencies around the world, you will see that they are all implementing RFID chips on items and increasingly on people.

The recent growth of the RFID industry has been staggering: From 1955 to 2005, cumulative sales of radio tags totaled 2.4 billion; in 2007 alone, 2.24 billion tags were sold worldwide and analysts project that by 2017 cumulative sales will top 1 trillion–generating more than $25 billion in annual revenues for the industry.

We're starting to see chips being implemented in credit cards, debit cards and passports, driver's licenses, health cards, and many other things. Increasingly they are being used to monitor people as well as items. RFID tags embedded into clothes and personal belongings allow people to be tracked and monitored in shopping malls, libraries, museums, sports arenas, elevators, and restrooms. American Express has them on their blue cards. They are announcing plans to place people-tracking readers in stores to track customers movements and observe their behavior. If you bought something with your credit or debit card, they will know what items you bought and if the items were chipped, they will know what you were buying. In this way they will be able to track you.

In 2006, IBM received a patent approval for an invention called, "Identification and tracking of per-

(continued on page 9)

sons using RFID-tagged items." One stated pur-

was to collect information about people that could be "used to monitor the movement of the person through the store or other areas."

When somebody enters a store a reader "scans all identifiable RFID tags carried on the person," and correlates the tag information with sales records to determine the individual's "exact identity." A device known as a "person tracking unit" which then assigns a tracking number to the shopper "to monitor the movement of the person through the store."

If I had three readers in this room, I could scan everybody in one second and I would know right away who's here; so it would scan that quickly. The computers are getting quite sophisticated and capable of doing large numbers of scans at any given time. One company recently announced a computer that reads data transactions at 200 million seconds, an incredible number.

Here's an example of how they are being used in companies; a few oil companies have given their employees smart cards so that they know where they are at any time of the day. This ensures that people do not go where they are not authorized to go. They will see how many times an individual might go to the washroom or outside to have a cigarette; things like that. It allows continuous tracking of people, and so more and more companies are thinking it's a novel idea.

In early 2007, the American government complained to the Canadian government that they were tracking American contractors who were visiting Canada by placing loonies ($2.00 Canadian coins) with tiny RFID transmitters in their pockets. And a CIS officer when confronted with this said: "Ah, give us a break! You might want to know where the individual was going, what meetings he's attending, who he's talking with and everything like that." So if they wanted they could track people with chipped loonies.

The University of Washington students, faculty and staff are being tracked as they move around the site so the details of where they've been, what they're doing and with whom, will be stored in their database. One of the professors at the University was asked, "Will you check on this student?" so he checked on him and said, "Oh, he's on the fourth floor just standing outside room 452 and now he's moving into the classroom."

In London you can buy a monthly pass to the transit cars that have an RFID on it and if you link the bus pass to a person's name you can track where this person is on the bus and subway system throughout London, England. Last year the police were getting four requests a month and now they are getting close to 100.

Just last week the London police announced that they were putting RFID chips on all of the 31,000 police in London. Now this may be on their ID card, they did not say if they were going to put them directly on their body, but they were getting chipped; it was published in the Daily Mail. Some of the police were complaining that they "are going to know where we are at any time, we won't be able to go into a coffee shop and get a donut." All 31,000 police in London now have RFID's so if they ever need to stop or control people they can direct 1,000 troops immediately to the scene.

In Southern China they're implementing RFID readers in the city of Shenzhen to track the movement of citizens; all citizens have an ID card with a chip so they can identify who is in what part of the city at any point in time.

The chips and National ID cards that they are trying to bring in now contain not only a number, but also a person's work history, education, religion, ethnicity, police record and reproductive history. The United States has been trying to implement the National ID card for a few years now and there are strikes going on in different states as they try to resist this National ID that will identify everyone in the country.

RFID readers in a library

Canada is adding a Real ID to the license plates and we don't hear anything about it, its being done a lot more secretly than it is in the States where there is a lot of public debate. The increase of the use of RFID chips is going to require a increased rate of the UBF spectrum, as a result in the United States they're going to stop using the UBF spectrum of the VHF frequency in 2009 and everything is going to go digital. You may have seen that on television in the United States.

Canada is going to do the same thing, they'll say it still works, and instead of the antenna on your roof you'll use a black box. The reason they're doing this is that the UBF and VHF analog frequency are being used for the chips, so they don't want to overload the chips with television signals, because the chips signals will now be receiving those frequencies.

A friend of mine from Quebec says his cows have a chip embedded under the skin. All farm animals have to be chipped and he says he's no longer allowed to kill as many cows as he wants. He was given a limit of two cows that he could kill and use only for the farm. All the others had to be sold to particular companies who could control those cows and get food from them. So he could only kill two and the others he had to sell to a supermarket chain.

People are being chipped now. There's a trend that they're promoting in the media in terms of chipping people; they're saying why not chip children for safety, so we can protect them, especially if they're in the hospital then nobody could steal the newborn babies. Why don't we chip the sick, then if someone has a heart attack and falls on the floor, we can read the signal in the chip and send someone to help them. We should chip the military so we would be able to know where the soldiers are and if they're alive. After we could chip people on welfare so we could make sure they're not cheating the government. Then we can chip all the criminals so that we could control them, and we'll chip workers because a lot of them goof off at work. Then we'll chip all the pensioners because they're just taking money from us; and after that we'll chip everyone else.

Some 800 hospitals in the United States are now chipping their patients. You can turn it down, but it's available. Four hospitals in Puerto Rico have put them in the arms of the Alzheimer's patients, and it only costs about $200 per person.

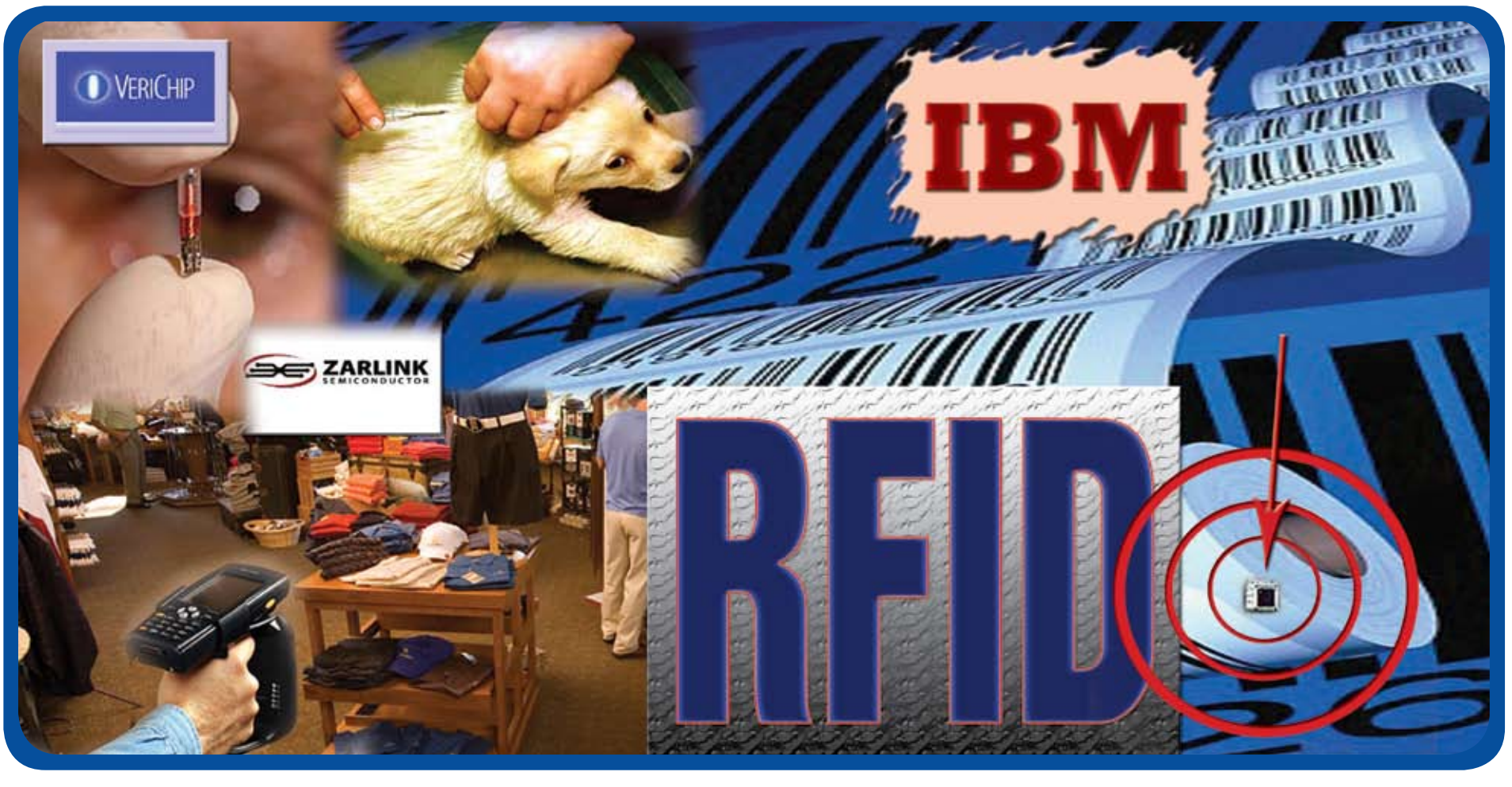
The Baja Beach Club in Barcelona gets patrons chipped. A BBC reporter went the club and got himself chipped. He said it was like getting a needle in your arm; they just rubbed it with some antiseptic and put a chip in. Because it was fairly small, he said it didn't hurt too much and he had it inside him so whenever he ordered he would just move his arm and pay for it. The reader on the bar would read the signal and since he had his bank account information on the chip on his arm it would deduct the money from his bank account.

Nigel Gilbert of the Royal Academy of Engineering said that by 2011 you should be able to go on Google and find out where someone is at any time from chips on clothing, in cars, cell phones, and inside many people themselves.

Chips are becoming more and more sophisticated. Nature Magazine reported recently that a drug containing microchips has been developed that will release drugs at the right time and amount. They can put a chip in you and release drugs so you don't have to take a pill every day. This particular one that they're selling lasts for over 140 days, you just have to get chipped three times a year with this drug and it releases it every day automatically. We will probably start hearing more about things like this in the near future.

In 2006, LifeScience.com said that European researchers have developed neuro-chips, they've coupled together living brain cells in silicone circuits and done a lot of experimentation on rats and snails. An electrical signal from a neuron is recorded in the chips transistors, while the chip's capitulators stimulate the neurons. They can create neuro-stimulators and use them to alleviate pain and lessen the debilitating effects of Parkinson's disease.

(continued on page 10)



An Introduction to New Technologies

(continued from page 9)

There are gastric stimulators that can treat obesity, they would make you feel hungry so you wouldn't want to eat anymore, it would just be necessary to put a chip in your brain that would connect and send signals. In another study, neuro-chip implants were developed and are being used on violent prisoners. They were implanted with the microchip (but they didn't know they were implanted), and when the implant was set at 160 megahertz's all the subjects became lethargic and slept about 22 hours a day. The implants ended all aggression in violent prisoners. Another interesting application is a silicone chip implant that mimics the hippocampus, the area of the brain known for creating memories. If successful, the artificial brain prosthesis could replace its biological counterpart, enabling people who suffer from memory disorders to regain the ability to store new memories. It's being developed by Professor Berger at the Center for Neural Engineering at the University of Southern California.

The mu chip is only .05 ml in length

They're working on rats and monkeys, so if applied to humans what this could do is restore your short-term memory which people lose as they get older, or it could replace your existing short-term memory with artificial short-term memory.

Applied Digital Solutions has a Verichip that is compatible with human tissue and can be used on implantable pacemakers or put defibrillators in artificial joints. It can be injected using a syringe and used as a sort of bar code in security applications. That's seen as one of the easy ways to implement chips in people through injections. They could very easily inject it via a flu shot or a vaccine.

Verichip is working on a glucose microchip that would determine glucose levels. You wouldn't have to draw blood to monitor glucose level. All you need is to have the doctor read your chip and your information and tell what your blood levels have been for the past month or two.

IBM has demonstrated a tiny device that measures heart rate and is able to sense when a person wearing it is in distress, after which it will call a cell phone for immediate help. The distress signal is sent wirelessly via Bluetooth.

Zarlink has developed the first swallowable camera capsule which uses Zarlink's RF transmitter to relay real-time images from the gastrointestinal tract. Our MICS (Medical Implant Communication Services) platform is designed with in-body communication systems that will improve patient care, lower healthcare costs, and support new monitoring, diagnostic and therapeutic applications.

Currently the chip uses 100 hair-thin electrodes that sense the electro-magnetic signature of neurons firing in specific areas of the brain in, for example, the area that controls arm movement. The activity is translated into electrically charged signals and are then sent and decoded using a program, which can move either a robotic arm or a computer cursor. According to the Cyberkinetics' website, three patients have been implanted with the BrainGate system. The company has confirmed that one patient (Matt Nagle) has a spinal cord injury, while another has advanced ALS.

This shows that human thoughts can be converted into radio waves and used by paralyzed people to create movement.

Matt Nagle sends the thoughts to a computer to decipher. He can turn his TV on or off, change channels, and alter the volume. (BBC 2005) He can also move his arms and pick up things.

In addition to real-time analysis of neuron patterns to relay movement, the Braingate array is also capable of recording electrical data for later analysis. A potential use of this feature would be for a neurologist to study seizure patterns in a patient with epilepsy.

Braingate is currently recruiting patients with a range of neuromuscular and neurodegenerative diseases, so if you want a computer chip in your brain you can just go on the website and volunteer.

What are the problems about these new technologies? Let me just give you a brief explanation. Chips are going to end privacy. There's a website called Spychips.com operated by Katherine Albrecht; they research the use of RFID's by different companies. They have been warning people about them because chips that have economic or health data could get that data stolen.

The New York Times in October of 2006 said that any card that doesn't require swiping (in other words that doesn't have a chip in it), is vulnerable to un-authorized charges and put people at risk for identity theft. You can buy scanners in electronics stores for $60 or more that can read the information on the chip.

They are finding that once implanted in people, chips can be damaging to our health. For example, the body of a rodent who was tested started rejecting some chips and started a development of cancer. Also there is a danger of viruses; you are all familiar with software viruses on your computers, imagine if you got a virus in your chip that deletes your information in your chip.

If chips can disseminate medicine then they can disseminate other things too; anything put inside a microchip can be activated by a signal. And finally, with this technology, subliminal mind control becomes possible. I went on to Google and did a search on mind control; you might find it interesting to check that yourself. I read one on patents; there are patents that exist for mind control. This is what one states: non-aural carriers, in the very low or very high audio frequency range or in the adjacent ultrasonic frequency spectrum, are amplitude or frequency modulated with the desired intelligence and propagated acoustically or vibrationally, for inducement into the brain. This is patent number 5,159,703 1992.

Another explains a device that can be placed in the auditory cortex of the brain. This device allows the following process: someone speaks into a microphone, the microphone then has the sounds coded into microwaves which are sent to the receiver in the brain and the receiver device will transform the microwaves back so that the person's mind hears the original sounds. In other words, a person with this device in their head will hear whatever the programmers send via microwave signals. (Phillip L. Stoklin took out patent number 4,858,612 on this.)

What do things like this mean to people of faith? You know from the Apocalypse, which is the last book of the Bible, that microchips are unacceptable to God.

Chapter 13, Verses 16-17: "And he (the beast) shall make all, both little and great, rich and poor, freeman and bondmen, to have a character in their right hand, or on their foreheads. And that no man might buy or sell, but he that hath the character, or the name of the beast, or the number of his name."

Chapter 16, Verse 2: "The first angel poured out his vial upon the earth, and there fell a sore and grievous wound upon men who had the character of the beast; and upon them that adored the image thereof."

Chapter 20, Verse 4: "And I saw seats; and they sat upon them; and judgment was given unto them; and the souls of them that were beheaded for the testimony of Jesus, and for the word of God, and who had not adored the beast nor his image, nor received his character on their foreheads, or in their hands; and they lived and reigned with Christ a thousand years."

If people have chips they will be tracked wherever they are. And there is a reasonable expectation that their bodies will be controlled and manipulated, as this technology is increasingly refined. Their minds will also be manipulated, they can certainly be made or induced to follow whatever people want them to follow. It's quite conceivable that they could be made to denounce God also.

□

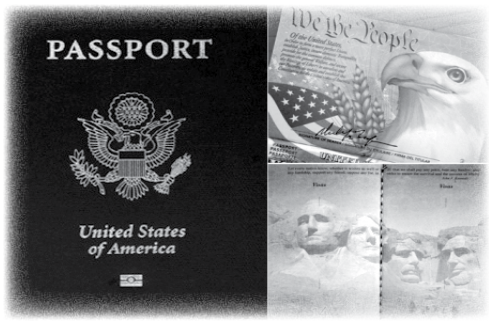
Patrick Redmond

RFID's in passports: facts you should know

Is there a difference between RFID-based ID cards and Homeland Security's new driver's licenses? The evidence would seem to say so. Other countries' national IDs and e-passports are using RFID tags that meet industry standards that are known as ISO 14443. This is being used only for the identification and payment cards, and has a prominent level of security and privacy protection installed in it. On the contrary, the U.S. border cards use an RFID standard known as EPCglobal Gen 2; this is a technology that was calculated to track goods in warehouses, where the objective is not security but greatest ease of readability.

Where the ISO 14443 standard has elementary encryption and requires tags to be close to a scanner in order to be read (a distance measured in inches rather than feet), Gen 2 tags characteristically have no encryption and negligible data safeguards. To browse the data from an encrypted ISO 14443 chip, you would need to uncover its encryption code, but no unusual knowledge is needed to skim a Gen 2 tag; the only thing you need is a Gen 2 reader.

Readers such as these can be purchased anywhere and indeed are used in warehouses all around the world. What could prevent any hacker or criminal with a bit of knowledge of computers to scan a border card from across a room, straight through a purse or even through a wall?



In China the amount of personal information that is encoded into their ID cards is enormous; they include health and reproductive history, employment status, religion, ethnicity and the name and phone number of the person's landlord. Worse still, these cards are only part of an even larger scheme to cover the cities in China with high-tech surveillance. China Public Security Technologies, which is a confidential firm that provides RFID cards for this endeavor, was described by its vice president Michael Lin as "a way for the government to control the population in the future."

A United Nations agency called the International Civil Aviation Organization (ICAO), whose function is to direct world passport regulations, has approved the production of RFID's in passports. ICAO now has decreed the endorsement of all such scannable "e-passports." Now almost every country in the world requires RFID passports, and as we know, that includes the United States.

These new passports have caused quite a commotion since they were first introduced, both on the privacy and security level. Even so, an ICAO official reported in 2006 that new encryption policies would exercise a "level of protection (that) should reassure the most anxious passport holder that his personal data cannot be read without his knowledge."

However, experts in security have said that the contrary is true. In 2007, a British security consultant named Adam Laurie, broke an encryption code on a U.K. passport and read the personal information that it contained – all while it was sealed in its mailing envelope! At about the same time period, German security consultant Lukas Grunwald copied data from a German passport's embedded chip and encoded it into a different RFID tag to create a forged document that could fool an electronic passport reader. Investigators from the Charles University in Prague, found similar vulnerabilities in Czech e-passports and stated that it was "a bit surprising to meet an implementation that actually encourages rather than eliminates (security) attacks."