computers are bad

You are receiving this facsimile because you signed up for fax delivery of this newsletter. To stop delivery, contact Computers Are Bad by email or fax.

https://computer.rip - me@computer.rip - fax: +1 (505) 926-5492

2022-07-21 preventing loss dot jpeg

Long time no post, or at least it feels that way! I have returned from a long vacation in a strange foreign country where the money is made of plastic, and I am slowly recovering from the tactile disturbance this caused. As tends to happen I ended up thinking a lot about the small details of international interoperation, and the issue of currency is an interesting one. I think my next post will be a bit about the mechanics of the relatively seamless ability to spend US funds in Canada or Mexico today. But first, a post that I started before I left and didnt finish until now...

EAS

You know how sometimes when you leave the grocery store, an alarm goes off which is either completely ignored or immediately reset by staff? Whats up with that? Well, I can only really offer a satisfying explanation of the *how,* as the *why* is a topic of some complexity.

The whole world of tag-detection-based anti-theft technology can be broadly referred to as Electronic Article Surveillance, or EAS. One of the tricky things about understanding EAS is that, much like with proximity key systems, several significantly different technologies are in use simultaneously. There are a lot of urban truths about EAS that are often correct insofar as they apply to one particular EAS technology, but often not even one of the more widely used ones. The different practical and security properties of EAS systems are interesting from an evolution of technology perspective, and the cutting edge of EAS gets into some interesting areas of RF engineering.

The general principle of EAS is fairly simple: article tags are affixed to, or placed in, products that might be stolen. At the exits of a retailer, a portal system is installed that detects the tags. When an item is sold to a customer, a cashier uses some mechanism to either remove or deactivate the tag so that the customer can exit without causing the portal to alarm. Whats less simple is the number of different ways of achieving this.

EAS systems are commonly, but mostly incorrectly, referred to as RFID. In fact, the most commonly deployed EAS use a technology which is quite dissimilar to RFID and relies on magnetic, rather than electric, field coupling. This makes it all the more interesting that EAS started out on the path to RFID, before taking rather substantial detours into the world of magnetics.

Minasy

There seems to be some confusion in common sources about the nature of the first EAS, although its agreed to have been invented by Arthur Minasy in the mid 60s. Its actually not at all difficult to find the original patent granted to Minasy in 1966, in between Minasys many other forays (he was the type of serial inventor which is rarely seen today). The original Minasy design, commercialized by a company he founded called Knogo, is a simple passive circuit that receives RF energy via an antenna, rectifies it to DC, and uses that to power an oscillator that emits RF at a different frequency. This is, of course, substantially similar to the RFID concept and I find it likely that Minasy would be listed today as among the significant contributors to RFID were it not for the fact that this original technology was quickly abandoned by Knogo and is little known today. This is true to such an extent that articles about the history of EAS, if they go into any real detail on early systems, tend to describe the *replacement* of the Minasy system as Minasys original invention.

There is a fundamental problem with both Minasys early design and modern RFID in EAS applications: it requires electronic components, and electronic components are expensive. This was true in Minasys day when individual transistors were a meaningful impact on the BOM cost, and it remains true today when EAS tags are made in tremendous volumes and fractions of a cent make a major difference.

The Minasy system, often called RF tags or resonant tags, are still in use today. The relatively high cost of the tags tends to limit them to applications where they can be reused, mostly in the form of hard tags attached to clothing and removed on sale using a special tool. That said, it is possible to deactivate resonant tags. LC tags can be manufactured with an intentional susceptibility to failure when exposed to an excessively strong RF field, for example by using a capacitor which will overheat and allow the plates to short together. The tags can then be placed on a device which emits the same frequency as the detectors but at a much higher power level, resulting in intentional failure of the tag.

A more recent (but not very recent) innovation is thinner and cheaper RF tags operating at a higher frequencytypically 8.2MHz, while the original Minasy system had been tuned for 2MHz with very low precision. These 8.2MHz tags look like rectangular thin paper stickers, and when peeled up the metal foil antenna is visible underneath. They operate on the same principle as Minasys system but are almost always deactivated by RF field rather than removed. Their thin size makes them well suited to printed materials, but they can also be applied to boxes and other packaging.

Magnetics

Far more common today than RF tags are a later development, the magnetic EAS tag. Magnetic tags exist in two major variants, the first having been developed by 3M in 1970. The 3M technology, commonly known by its 3M brand name Tattle Tape, can more generically be called electromagnetic or EM EAS. EM tags rely on an interesting property of magnetic fields, or rather their interaction with magnetic materials.

Magnetic materials such as iron can be magnetized by exposing them to a magnetic field, causing an alignment of the magnetic dipoles of the materials molecules. During this process some of the energy of the field is consumed. Magnetic materials also have a saturation value, which is a measure of their greatest potential to become

magnetized, or the point at which no further improvement in the magnetization of the material can be achieved. For most magnetic materials, the saturation value is quite high. It is possible, though, to design materials that are magnetizable but have a very low saturation value. The most common in EAS applications is an alloy called metglas, so called because it has a non-crystalline structure more similar to glass than metal.

When a quantity of metglas is placed in a magnetic field, it absorbs some of the energy of the field in order to become magnetized. It quickly reaches saturation and stops interacting with the field. This behavior is quite useful as it can be detected by magnetic means.

So, an EM EAS system relies on a portal with two antennas, typically placed on the two sides of the door (in multi-door situations it is common to have multiple towers which alternate receiving and transmitting). The transmitting antenna emits a magnetic field. The receiving antenna on the other side of the portal observes this field. When metglas is introduced into the field, it briefly absorbs energy and then stops when it reaches saturation. This can be observed as a brief dip in field strength at the receiving antenna. By rapidly alternating the field emitted by the transmitting antenna (essentially using it as an AC electromagnet), this effect can be checked for many times a second.

Even better, the nonlinear behavior of metglas in a magnetic field causes a number of effects in a rapidly alternating magnetic field including harmonic frequencies resulting from the repeated magnetization and demagnetization of the metglas. Modern EM EAS systems use complex DSP techniques to observe for multiple different effects caused by the low-saturation-value material, making them less susceptible to false positives. In fact, false positives in the detection of metglas are quite rare (although EAS are usually quite prone to false positives, they come from other causes which we will discuss later). Because materials with a very low saturation value are exceptionally rare in nature, the presence of rapid magnetic saturation behavior is a very strong indication of the presence of a tag.

Magnetic EAS technology becomes even more interesting when you consider the issue of deactivation. EM tags are typically manufactured with a strip of a normal ferromagnetic material placed alongside the metglas strip. If this material is magnetized, it keeps the metglas strip constantly saturated, preventing it interacting with external fields. Thus an EM tag deactivator simply emits a strong enough field to magnetize the ferromagnetic strip. Even better, an activator can emit a rapidly alternating magnetic field which will effectively scramble the magnetic orientations of the underlying magnetic elements in the magnetic strip, causing it to lose its magnetic field. The metglas strip will no longer be held in constant saturation and will be detected as usual.

This ability to activate and deactivate EM tags at will is unique to EM tags and is the cause of their ongoing popularity in libraries. Libraries install tattle tape permanently, usually adhering it to a middle page near the spine where it is difficult to notice. The circulation desk deactivates tags when books are checked out and activates them when books are checked in, usually using a device that just has an activate/deactivate switch to select between a fixed and alternating magnetic field.

If this neat property of EM tags seems a little too good to be true, well, it does have caveats. First, the ferromagnetic element in EM tags is of relatively low coercivity (e.g. magnetically soft) to allow for easy activation and deactivation. That also makes it prone to being affected by various environmental magnetic fields,

and as a direct result EM tags have a tendency to self-activate over time. If you have ever renewed a library book a few times and then set off the door portal when returning it, this is due to the ferromagnetic element simply losing its magnetization over weeks of exposure to electrical equipment and other ferromagnetic materials.

Second, the only aspect of EM tags that can be detected is the presence of an active one. There is no way to differentiate EM tags from each other. This can be a practical problem in circulation environments like libraries. In my city, the county library has ended use of EM tags in favor of an RFID system, but much of their inventory is still tattle taped. The tags in these older books are now almost all active due to environmental demagnetization, and so it is more or less guaranteed that carrying a county library book into the university library will set off the portal system... on the way in and out. This kind of nuisance alarm behavior will very quickly cause staff to disregard the EAS system, and so the county librarys upgrade to RFID has no doubt significantly reduced the effectiveness of the university librarys system.

EM tags are most often seen in the form of tattle tape, whether made by 3M or a competitor. These tags are long, narrow strips that are usually self-adhesive. They are thin enough to sit inconspicuously in the pages of a book, but large enough that they would be tricky to get onto the packaging of smaller products. You dont see them very often, mostly because in their most common application of library books theyre placed either in the spine or on a page very close to it, where theyre concealed.

EM tags cannot really be permanently deactivated without physical destruction, and they require relatively strong fields to detect. These two downsides lead to the development of a variation on magnetic EAS, called AM EAS. The label is a little confusing here as most would read AM and assume amplitude modulation, but in this context its actually an abbreviation for acousto-magnetic. These tags rely not just on the interaction of a material with a magnetic field, but also on acoustic resonance of the material. Thats pretty neat.

AM tags contain a thin strip of a material that demonstrates magnetostriction, or a change in physical shape when exposed to a magnetic field. They are sized such that they are resonant when vibrated at a particular frequency, usually 58KHz. The AM portal system emits short bursts of a 58KHz field and then, after transmitting, uses a receiving antenna to observe for any continued 58KHz magnetic oscillation. An AM tag will continue to vibrate for a short time after the original field disappears, causing a detectable trail from the transmitted burst. Once again, modern portals repeat this process rapidly and use DSP methods to check for multiple indications of a real tag.

AM tags can be deactivated much like EM tags, but there are important differences. AM tags also contain a strip of a ferromagnetic material, but its function is different. The ferromagnetic strip is magnetized normally and serves as a bias magnet. As a bias magnet, it is carefully tuned so that it offsets the magnetic anisotropy of the magnetostrictive stripits tendency to only react to magnetic fields coming from one direction. Without this bias magnet, the AM tag cannot be reliably detected. To deactivate AM tags, the magnetic strip is demagnetized by exposing it to a strong and alternating field. AM tags are the opposite of EM tags when it comes to activation and deactivation, and so they have a bias towards deactivation. This bias is weak though: the proximity of the bias magnet to the magnetostrictive strip and the inconsistent placement of these tags makes it impractical to remagnetize or reactivate them, so theyre designed for one time use only. This means that the ferromagnetic material used for the bias magnet can be of relatively high coercivity and is less affected by normal environmental fields.

Ill go into a little bit more depth on typical AM equipment, because AM is the most common EAS technology used in US retail. Virtually every retailer has at least AM portals, and you have certainly seen AM tags. AM tags are relatively thick but small compared to EM tags. Theyre usually in a plastic housing of perhaps 4cm long (as common as they are I couldnt find one around to measure) and a few mm thick. The largest manufacturer of AM tags is Sensormatic, and so they often have the old hand in crosshairs Sensormatic logo printed on them.

AM tags are ubiquitous in part because they are the accepted technology for source tagging. Source tagging is a common industry convention in which anti-theft tags are placed in products by the original manufacturer rather than the retailer. There are a few advantages to source tagging: not only does it save labor on the part of the retailer, the manufacturer can usually place the AM tag in a more discrete and difficult to tamper with location. For example, its very common for power tools to come from the manufacturer with an AM tag inside of the tool, often adhered to the inside of the plastic molding for the handle. I recently encountered an item of clothing with an AM tag sewn into a label, although fortunately this practice isnt common... AM tags are quite rigid and not especially comfortable to wear.

Source tagging also allows for the use of EAS throughout the supply chain. Fulfillment and shipping warehouses, for example, can use AM portals to deter theft by employees, even before delivery to a retailer.

AM deactivators consist of a large coil antenna, which may be constantly active but on modern equipment usually runs in a low-power detection mode where it behaves similarly to a portal. The coil only runs at full power to demagnetize when it detects the presence of an AM tag. This saves a bit of money on electricity but more importantly makes the deactivator less likely to deactivate someones credit card, which had been an occasional problem with AM deactivators despite the high coercivity of payment card magnetic strips. Some AM deactivators, probably those that have received some physical abuse, demonstrate magnetostriction of the coil itself in the form of an audible ping or twang each time the coil is powered [1].

AM portals are the most common type you see. Older AM portals (and EM portals as well) sometimes stayed unpowered until they were activated by a pressure-sensitive mat or deck between the antennas, and you might still see this in libraries in particular where continued use of EM gives little motivation to upgrade equipment, but most portals today are able to use electronic and DSP methods to detect the possible presence of tags with a very low power consumption. This sometimes takes the form of search and interrogate modes (these terms are often used in remote sensing due to its military origin and so I tend to use them), where the portal normally operates in a low power mode and the detection of any kind of magnetic interaction causes the portal to switch to a higher power mode to distinguish tags from ordinary metals.

Sensormatic is the largest manufacturer of AM portals as well as tags, so you will likely recognize the Sensormatic product lineup that varies from big beige towers to clear lexan sheets with coils embedded in them. Newer portal systems are relatively small, and Sensormatic even offers a concealed option that mounts against the door frame (not really very discretely at all) instead of requiring freestanding towers for the antennas. Of course it is limited to a fairly short range due to the small size of the antenna coils and so it doesnt seem to be that common. A more recent innovation is the installation of surveillance cameras either on the antennas or at the door frame. Sensormatic controllers can trigger video surveillance systems [2] or retrieve images from a video surveillance system, either way offering correlation of detection events with video of the person walking through.

While AM portals are mostly effective and extremely common, they do have distinct downsides. They share with the EM the property that AM tags cannot be differentiated. A common downside emerges with source-tagged items: if you purchase a source-tagged item at a retailer that does not have an AM portal, they will likely not deactivate the tag on sale. It will then set off the portals at other retailers. This is an extremely common cause of false-positive alarms. The portal also cannot indicate how many items or what types of item were detected, which makes it difficult to investigate an alarm.

As a partial mitigation, vendors including Sensormatic now offer handheld wand AM tag detectors with a short range. These can be used much like a wand metal detector to identify the item, or at least location on the body, that triggered the alarm. WalMarts are usually equipped with one of these in a wall-mount charging cradle near the door, but I have never actually seen one used, which foreshadows a later point Ill discuss.

Another downside is the size of AM tags. Theyre not exactly large, but they are thick... too thick to be easily integrated into some types of packaging. Their larger size also makes them easier to locate and remove, if theyre not hidden somewhere by source tagging. Retailers that apply AM tags to items will sometimes apply a larger sticker with anti-removal features (scoring so that it will not peel away in one place) to frustrate shoplifters that simply peel off the tag, but of course this isnt entirely effective.

RFID

As I mentioned, genuine RFID has been applied to retail EAS. It remains relatively uncommon because, despite advances in low-cost manufacturing of small electronics, active RFID tags remain considerably more expensive than AM tags.

Perhaps the greatest champion of RFID EAS is WalMart, which has invested considerably in both the installation of RFID equipment (manufactured by Sensormatic) and the standardization and promulgation of RFID Electronic Product Code or EPC tags. Much like UPC (Universal Product Code) or the closely related EAN (European Article Number), EPC is an effort to assign a unique numeric ID to every product in a retail environment... but EPCs tend to be more specific than UPC, to the SKU (stockkeeping unit) level rather than price level. This means that products that are offered in multiple variations (e.g. flavors) at the same price may share the same UPC, but will have distinct EPCs.

One of the driving motivators behind this technology is its advantages for inventory management. In order to effectively track shrink (theft, spoilage, loss, damage, etc) and other dispositions of purchased inventory other than sale, retailers need to actually count the inventory on the floor. This is also a required step in financial auditing, insurance underwriting, and various other business processes. Basically, large stores need to actually send people out to count everything.

In practice retailers rarely handle this in house, particularly because the auditing use of this information makes it valuable to have it collected by an independent third party. For example, the use of an inventory contractor makes it more difficult for an insider (employee) who is stealing products to cover for the loss by inflating inventory counts. The largest such contractor in the US is a company called RGIS, which regularly sends an army of temp workers equipped with handheld barcode scanners

into each of Americas stores in order to scan every individual item on the shelves.

Sidebar which is Critical of Capitalism, You Have Been Warned

Actually the history of retail inventory is itself rather interesting as RGIS has historically been a pioneer in the design of highly usable wearable computers, and in the era before the universal use of UPC/EAN labels the incredible speed at which experienced RGIS employees could operate a belt-worn ten-key was something of a legend. Of course in one way, the invention of the barcode was a labor-saving device that ought to accelerate the inventory process greatly.

However, as potently observed by Brian Justie in The Nonmachinables (Logic Magazine), many automation technologies are better viewed as labor technologies in that their primary purpose is not actually to speed up a process but to reduce the level of operator skill required, thus making the labor more readily replaceable. This phenomenon is rather clear in the case of RGIS, where more than speeding anything up the transition to barcodes facilitated RGISs transition to nearly complete use of short-term temp agency employees.

Since RGIS workers no longer needed to learn the skill of rapid and accurate manual entry, they no longer needed to be paid at a level that motivated them to stick around. Anecdotally, it seems that the modern barcode-based RGIS system is quite possibly slower than the earlier belt-pack ten-key, but the operator only needs the barest of training and therefore only the barest of pay or benefits. This is one of numerous cases in which advancing technology has reduced costs as promised, but *by facilitating lower wages, rather than by actual improvements in efficiency*.

End of leftist discourse

The EPC scheme promises to significantly accelerate the inventory process by allowing drive-by inventory with a good sized antenna. It also offers a significant enhancement in EAS: an EPC-based EAS system can determine exactly which items are detected and report the list of items to the operator. Even better, EPC can include a unique serial number for each item. This way, deactivation of the tag can be performed in an online manner by marking that individual item as sold. This promises significantly more accurate EAS, easier investigations of alarms, and better overall inventory control and market research insight via end-to-end lifecycle tracking of individual products.

It is also, according to a surprisingly large segment of the American population, a sure sign of the coming apocalypse. Im sort of kidding about this but only sort of. A meaningful vein of opposition to RFID technology in public discourse has been its potential resemblance to certain aspects of the Book of Revelations. To discuss this fascinating and surprisingly important artifact of American culture would be its whole own article, but I will note the comedy of Not Today Satan Cross Christian Religious Credit Card RFID Blocker Holder Protector Wallet Purse Sleeves Set of 4 listed on WalMart.com coming up in the same search results as ALERT, RFID CHIP READER IS AT WALMART THE MARK OF THE BEAST IS HERE IN VIRGINIA.

A much larger problem with RFID than its satanic origins remains the cost of tags, which has lead to a lot of hesitation on the part of manufacturers and distributors to participate in RFID source-tagging schemes. WalMart is of course a large enough part

of the US economy that it has a powerful ability to push its suppliers around, and WalMart just recently announced that it will mandate source-tagging with EPC for a large portion of their products. This needs to be done at the expense of the supplier, of course, although WalMart notably continues to exclude groceries from the requirement. The required categories for EPC tagging are basically all higher-value and higher-theft products, showing the practical impact of the tag cost. This same trend is seen throughout the world of EAS: the cheaper and less attractive to thieves an item is, the less likely it will have any sort of tag. The more expensive or theft-prone an item, the more likely it is to feature AM and then RFID tagging.

Although the expansion of EPC tagging at WalMart is recent, the system itself is not, and WalMart has used EPC tags on product cases and some apparel items since 2003. So have other retailers, although usually not on as large of a scale. The technology lead to enough debate around privacy (and rapture) implications that WalMart attempted to placate public concern through transparency by putting an EPC In Use decal on entry doors somewhere between the other ten regulatory decals. Of course this has never achieved any type of benefit, but I do like the design of the sticker.

Another stronghold for RFID EAS technology is the library industry. The same requirements that kept libraries on EM make RFID attractive, and so most libraries are transitioning from EM to RFID (or already have in the case of most larger libraries). Besides allowing for very accurate online tracking of checked-in/checked-out status of books, it speeds up the circulation desk (or self-service kiosk) by allowing a whole stack of books to be scanned at once. Since library books are fairly expensive and have fairly long service lives, the cost of the tags is not so much of a deterrent to libraries, and RFID tags are readily available in a thin sticker format the goes just fine inside the cover of a book.

Most RFID EAS tags are thin stickers made of either paper or plastic. Theyre often square or fairly close to square. Usually either peeling one up and looking underneath or shining a light through an RFID tag will reveal a spiral or otherwise packed antenna, similar to PCB traces but more often just a metal foil on a paper or plastic backing. Some RFID tags have a serial number or barcode printed on them, but many are just blank. In the case of EPCs on apparel, its common for the RFID tag to be adhered into the middle of a two-layer paper hangtag. Libraries usually put them inside of the front or back cover, and retail products often have them placed somewhere near the UPC/EAN barcode since this gives the cashier a good idea of which side of a large box to put against the reader.

RFID EAS portals are mostly not distinguishable from AM portals, since RFID support is usually just an add-on feature to an AM system (by adding extra antenna coils in the same tower enclosure). RFID EAS systems are a lot more likely to have some sort of operator interface like a display and keypad on the wall, rather than a simple alarm, since theyre able to show a list of items detected.

Unexpected part break...

This has already become quite long and I have quite a bit more to add... as sometimes happens to me, everything Ive said so far is really just background to what I really wanted to discuss. Lets break this up a bit by calling this part 1, and soon I will post part 2... which will cover both cutting-edge retail loss prevention technology and the reason why both existing and brand-new systems are increasingly ineffective. There will be more criticism of capitalism, but also more weird technology!

[1] Iron is slightly magnetostrictive and this effect is the source of a lot of cases where you can hear electricity. The 60Hz hum of large power transformers, for example, is primarily the result of the transformer windings vibrating due to magnetostriction.

[2] Support for external triggers is a longstanding feature in video surveillance systems, allowing video to be recorded on demand or just tagged with the time of events. In older systems this takes the form of a relay on the EAS system that energizes a digital input on either the video recorder or a camera (digital surveillance cameras usually include one or two digital input/output pins and a protocol to inform the recorder when their state changes). In newer systems it is more likely to be all IP.