Extreme-range RFID tracking

Chris Paget

ivegotta@tombom.co.uk / @ChrisPaget

Presented at Blackhat USA 2010, Las Vegas.

Synopsis:

If you think that RFID tags can only be read a few inches away from a reader you haven't met EPC Gen2, the tag that can be found in Enhanced Drivers Licenses - this 900MHz tag is readable from 30 feet with off-the-shelf equipment. Without amplifying the signal from a commercial reader I was able to equal the previous Defcon record of 69 feet, and with less than $1000 of equipment I achieved considerably further than that. This talk covers everything you'll need to know to read federally-issued RFID tags at extreme ranges and explores the consequences to personal privacy of being able to do so.

Intro to EPC Gen2

Most modern RFID systems work on the principle of inductive coupling: a coil of wire in the reader transfers power to a coil of wire in the tag using a magnetic field, in much the same way as a transformer. Magnetic fields are often referred to by ham radio operators by the name "Near Field" since field strength drops off very sharply with distance (as an inverse cube relationship) – this is usually the primary limiting factor on RFID read range.

Enter EPC Gen2. EPCGlobal is a worldwide RFID standards organization whose specifications cover the vast majority of tags issued in the 900MHz band. Correctly referred to as "Class 1 Generation 2", Gen2 is compatible with all previous classes and generations of 900MHz tags; more importantly though, it does not use a magnetic field to transfer power to the tag. Gen2 is much more akin to Radar than it is to more traditional inductive RFID; the reader is a "true" radio transmitter while the tags return data to the reader by changing how much of that transmission they reflect (i.e., they modulate their coefficients of reflectivity). Since Gen2 is based on radio and Radar technologies we can use techniques from these domains to drastically improve the range at which tags can be read; for an initial benchmark, a retail device will read tags at 30+ feet without modification.

Gen2 is a very active and widely-used technology. Gen2-compliant tags are currently being issued as part of the Western Hemisphere Travel Initiative; this includes the US Passport Card, the NEXUS, FAST, and SENTRI border-crossing cards, as well as the Enhanced Drivers Licence that is currently being issued by several US states and many Canadian provinces. Many supply chains also make use of Gen2; while Walmart is the best-known, many other retail chains are also deploying Gen2-based systems and it is fair to say that Gen2 is a common technology. Several high-level variants exist which offer minor improvements to the basic Gen2 specification but they are largely compatible with each other; any Gen2 reader should be able to read most Gen2 tags.

Radar, IFF, and the Radar Range Equation

Since Gen2 tags work in much the same way as Radar it is sensible to have an understanding of Radar to begin with. The word "Radar" is an acronym for RAdio Direction And Ranging; it works by bouncing radio waves off a distant object. A high-power transmitter (typically with a rotating dish) sends out a narrow beam of RF energy; by timing how long it takes for this energy to be reflected (and by knowing the direction the dish is pointing) it is possible to calculate the direction and range of the target object.

IFF (Identification of Friend or Foe) is a system built on top of Radar, sometimes called secondary Radar. While modern IFF transponders operate without Radar, IFF was originally designed to return data to a Radar ground station which identified the aircraft. This data was returned by electronically changing the efficiency with which the aircraft absorbed or scattered incident radio energy; by returning more or less of the signal to the ground station it is possible to transmit digital data. A good analogy is that of the plane itself – the plane can tip from side to side, controlling how much of the wing surface area is facing the radar station (and hence how much RF energy is reflected back). IFF does the same thing electronically; it is this mechanism that is used by Gen2.

Since the operation of Gen2 RFID is based on a Radar system, the same mathematics as Radar can be used (with some limits) to determine read range of Gen2-based system. Neglecting real-world effects for a moment, the purest form of this mathematics is the Radar Range Equation:

$$R_{max} = \sqrt{\frac{(G_r G_t \lambda^2)}{4\pi^2} \frac{P_r}{P_t}}$$

Source: ThingMagic (http://bit.ly/BKNOk)

In this equation:

Rmax is the upper limit on read range

Gr and Gt are the gain of the receive and transmit antennas

λ is the wavelength of the frequency in use

Pr is the power output from the reader

Pt is the threshold power at which the signal can be received (i.e., the sensitivity of the receiver)

I'll revisit what this all means later but for the moment it's important to note two things:

1. **Gen2 read range is derived from the square root of transmitted power**
2. **Gen2 read range is derived from the square root of antenna gain.**

In other words, if we increase either the output power of our transmitter or the directional gain of our antenna, we should expect to see the square root of that gain as a range increase. For example, if we go from 1 watt of RF power to 100 watts, we would expect to see a 10x increase in read range (10 being the square root of 100). Of course the real world is far more complex than this, but it's a good first-pass approximation. Clearly we can scale Gen2 read range by increasing both transmitter power and antenna gain; first we must define the mathematical relationships involved.

Decibels: dB, dBm & dBi.

This paper will assume that the reader understands the basic mechanics of decibels, which I believe is common among technical folk. If not, I recommend reading the wikipedia page; it explains them far better than I can.

Since decibels represent just the ratio between two quantities, it is sometimes useful to define one of those terms in a consistent manner. Power is typically represented in units of dBm, where the reference unit is 1 milliwatt. 1 watt of power then becomes 30dBm; one hundredth of a milliwatt becomes -20dBm, and so on. The gain of an amplifier (and the loss of an attenuator) are typically expressed in dB, so calculating an RF chain is reduced to simple addition and subtraction: 20dBm (a hundred milliwatts) into an amplifier with gain of 30dB (one thousand) becomes 20+30=50dBm, or one hundred watts.

Antenna gain is usually represented in terms of dBi, where the reference unit is an isotropic radiator – a so-called “perfect antenna” that radiates energy evenly in every direction. Antennas usually focus RF energy in specific directions; if you are standing in this beam looking at the antenna you will see a stronger signal than you would from the same transmission power into an isotropic radiator (since the radio waves are focused towards you). This is where antenna gain comes from; by focusing the radio waves in one direction the signal appears stronger. dBi is the gain that an antenna will give you compared to an isotropic radiator, again on the logarithmic decibel scale.

Combining these three units is trivial and results in a measurement called the EIRP – the Effective Isotropic Radiated Power. If we connect our previous 50dBm transmitter to a 10dBi antenna we get an EIRP of 50+10=60dBm, or 1 kilowatt – there's only 100 watts of power being emitted (or 100W PEP), but it would take 1 kilowatt of power into an isotropic radiator to achieve the same signal strength.

Ham Radio

In order to start running powerful transmitters into big antennas, it is essential to first obtain a license from the FCC. Amateur Radio (or Ham Radio) licenses are easy to obtain, with the examination questions published freely and a mere $15 to take the test. US amateur licenses come in three classes: Technician is the easiest with General and Extra coming afterwards. Each level confers additional transmitting privileges across the amateur bands while requiring additional knowledge to pass the test. That said, online study guides (such at that http://kb0mga.net/exams/) are easily enough for anyone who simply wishes to memorize the answers in a cram session. I'd recommend taking the time to actually read up on anything that you don't understand so that you can pass the exams from knowledge; you'll learn a surprising amount very quickly and will appreciate the extra knowledge when you come to put it into practice.

Gen2 tags operate in the 902-928MHz band under the FCC's Industrial, Scientific and Medical (ISM) rules. This band is not generally used by hams for exactly this reason (it's very noisy due to ISM) but it is nonetheless an amateur band; equipment is readily available to licensed amateurs in the US. By operating under ham radio rules we incur a number of technical rules, primarily:

- Restricted to 1500 watts of RF power (that's PEP, not EIRP).
- Restricted to 50 watts within 241km of White Sands, New Mexico (no kidding)
- No restrictions on EIRP or antenna gain
- Station must identify itself every 10 minutes and at the end of transmission.

There's a lot more restrictions but those are the essentials of the technical rules; we've got a 1500W maximum into as big an antenna as we can find, and we have to morse out a callsign every 10 minutes.

Stage 1: Antennas

An easy first step (and a good test of the Radar Range Equation) is to fit a commercial reader with larger antennas. Two yagis were purchased (one for the transmitter and one for the receiver); they were chosen to be as high gain as possible to yield the maximum return. However, since the RFID reader being used initially (a Symbol XR400) is an ISM-band device it is designed to reject foreign antennas; it does so by measuring the DC impedance of the output line. At radio frequencies the antenna has an impedance of 50 ohms, however a 10K resistor soldered inside the antenna provides an uncommon impedance for which the reader can check (a typical DC impedance for an antenna would be either open-circuit or short-circuit).

In order to bypass this protection, two steps were needed. First, a 10K resistor was soldered across the antenna connector inside the casing of the reader. This convinced the reader that a “legal” antenna was connected, making it constantly supply power to the port – this could be damaging if there is no antenna connected, so from this point on care must be taken not to power the reader on without an antenna. Secondly, the antennas chosen used a loop-type active element which at DC is effectively a short-circuit; this short-circuit overrides the 10K resistor and the reader again disables the port. For this reason a 902-928MHz ISM-band filter must be installed between the reader and the antenna; in addition to presenting the necessary open-circuit to the reader (which at DC will now only see the 10K resistor) this has the added benefit of reducing any out-of-band emissions.

Using these techniques and a pair of 13dBi yagi antennas (costing around $100 from http://bit.ly/cdelVf), I was able to increase the read range on a commercial reader from its standard 30 feet. According to what we learned from the radar range equation earlier there should be an increase in

range corresponding to the square root of the increase in antenna gain; since decibels are a logarithmic scale we can take a square root by simply halving. The stock antenna has 6dBi gain and I replaced it with an antenna that has 13dBi gain for an increase of 7dBi; when we halve this (to take the square root, according to the radar range equation) we should expect to see a range increase of 3.5dB, or a factor of 2.24. Given the standard read range of 30 feet (which we made sure to validate beforehand) this comes out to 67 feet; in my tests I successfully read tags in this configuration at a little over 70 feet. This will probably be the configuration used for the on-stage demo during Blackhat, where I'll hand out several hundred tags to test on-stage for you to verify in person.

While this is a convenient configuration technically, it is also somewhat breaking the rules. You shouldn't modify ISM-band equipment like this unless you're prepared to fully operate it under a new license (in this case an Amateur license), and that means that you need to identify the station every 10 minutes. This is virtually impossible for commercial ISM gear since it hops frequency too rapidly – this is required under FCC rules and prevents us from even being able to even tune in a second transmitter. Given this I took the only reasonable approach: kept on-air time to the absolute minimum that was required (often only seconds), kept transmission power to an absolute minimum (at all times measured to be less than the original output power of 1 watt), and used remote areas for testing wherever possible.

Stage 2: Transmitters and Amplifiers

At this stage I chose to discard the commercial reader, instead relying on a software-radio implementation using the USRP. The software at http://bit.ly/9FCDUv is both a Gen2 reader and a Gen2 sniffer implemented using GNU Radio; while the USRP is a general-purpose device and lacks some of the RF characteristics of the commercial reader, it does allow for precise control to be taken of the output frequency. I was able to use a second transmitter (tuned to the same frequency) to effectively overwrite the Gen2 signal at regular intervals, allowing me to identify the station and comply fully with ham radio rules.

The simplest transmitter I was able to find was an IM-ME, a $20 instant-messaging device aimed at tween girls which has become popular among hackers due to its wide functionality and lack of firmware security. Using a lightly-modified version of Travis Goodspeed's IM-ME morse code transmitter (http://bit.ly/ce3fwF), we created an automated callsign generator tuned to the same frequency as the USRP. While this complicated the RF chain somewhat (in order to match power levels between the USRP and the IM-ME) it did at least assure my compliance with FCC rules.

In order to ensure that the morse code from the IM-ME was stronger than the Gen2 signal from the USRP, I measured the output of both using a spectrum analyzer, yielding a figure of 5dBm for the IM-ME and 20dBm for the USRP. I therefore added a 16dB attenuator to the USRP output (bringing it to 4dBm, below the IM-ME) and mixed the two signals together using a standard power combiner. At this stage I had a combined signal that carries both the Gen2 signal from the USRP and a station ID from the IM-ME, at around 6dBm peak intensity (since the two do not combine exactly).

Now that my transmissions are correctly identified, I can introduce power amplifiers up to the legal limit of 1500 watts. To start with I purchased a 70 watt amplifier from http://bit.ly/dvhFNR for $400; in radio terms this is a significant amount of power and is easily capable of creating RF burns. It is also near the limit of my current antennas (100W) for a very reasonable price tag, but comes with a small problem. RF amplifiers do not generally come with volume knobs; in order to get maximum power out of an amplifier you must put a specified amount of power on the input, in this case 20mW (13dBm). Since our Gen2 driving signal is at only 4dBm this placed a significant limit on output power and therefore read range.

Solving this problem is relatively simple with another amplifier; $50 from http://bit.ly/bIfZJb buys a tiny preamplifier with 18dB gain, 16.5dBm output power, and frequency ability far beyond the 900MHz band in use. In order to saturate the power amplifier we require 13dBm output from the preamp; given its 18dB gain this means -5dBm at the input, or around 10dB less than the output from the power combiner. By adding and removing attenuators of various sizes beyond the minimum 10dB I was able to control the output from the power amp, allowing range to be incrementally increased as testing progressed.

Testing and Results

In addition to powering the tag, the reader must be able to receive a response from it. During testing, we noticed an interesting artifact that allowed us to easily determine whether the read range we had achieved was limited by the transmitter (i.e., not providing enough power to turn on the tag) or the receiver (i.e., not able to pick out the return signal from the noise). The two situations proved easy to tell apart due to the nature of the tags power consumption.

Like most silicon devices, Gen2 tags require an initial burst of electricity (known as startup current) to power on before dropping down to a lower operating power. Since the power available to the tag is directly related to the distance between the tag and the reader, by carefully controlling the tag distance at around the point where signal is lost we can distinguish two different situations:

- **Read range is limited by transmitted power**.

  In this case, the tag is unable to gather enough power to operate and switches off. It then requires a significant decrease in range to turn back on (to give it the necessary startup current), after which range can be increased again until power is again lost – it exhibits read range hysteresis.

- **Read range is limited by receiver sensitivity**

  In this case, the tag remains constantly powered and transmitting but travels in and out of range of the receiver. There will be a clearly-defined point beyond which the tag cannot be read, and before which the tag will always read – no read range hysteresis is present.

By examining the read range for hysteresis effects, it is easy to determine the effective limit to read range and compensate accordingly. In the first case simply adding output power will be sufficient; in the second case we found several solutions to be equally effective in different test scenarios:

- Add a low-noise amplifier (LNA) between the antenna and the receiver (increase the received signal strength)
- Add an ISM-band filter between the antenna and receiver / LNA (decrease out-of-band noise)
- Increase the receive antenna gain (limit the directions and polarizations that are received)
- Increase transmitted power (increasing the reflection from the tag)

There are other types of interference that we can do little to prevent technically, but can sometimes take procedural steps to remedy. These include:

- **In-band noise such as other ISM stations.** This can be reduced by choosing a location that is far from other ISM transmitters and relatively isolated (such as a canyon in the desert); also careful channel selection and filtering within the software radio implementation will greatly assist.

- **Receiver sensitivity** cannot be increased beyond a practical limit of around -110 to -140 dBm without extreme measures such as cryogenic cooling. While preamplifiers are useful up to a point (to improve on the sensitivity of the USRP), their returns diminish rapidly.
- **Transmitter crosstalk** is inevitable due to the nature of Gen2, in that it transmits and receives on the same frequency at the same time. This can be minimized by spacing antennas far apart and by carefully separating RF paths; it also helps to examine antenna plots to minimize off-axis lobes in critical directions. Beyond this there are some highly advanced analogue and DSP techniques that can be used to precisely pick modulated signals out of strong carrier signals; these are beyond the scope of this paper and a EE degree is recommended.
- **Clutter** is caused by reflections of the transmitted energy from other objects in the area that are not RFID tags, and even the atmosphere itself. As range is increased clutter also increases, eventually to the point where it entirely swamps the signal from the tag. Again, a clean testing environment is essential (with a large anechoic chamber providing ideal conditions).
- **Ground interference.** Some of the transmitted signal will inevitably be sent downwards towards the ground, to be reflected back up again at the tag (which will again reflect some down towards the ground). This multipath interference will cause a "blurring" of the signal at both the tag and the reader, eventually degrading it to the point where one or other can no longer comprehend. Increasing the height of the antennas above ground will decrease this effect, as will choosing a testing location with a conductive ground to absorb the downward energy (seawater is almost ideal).
- **Atmospheric effects** will degrade the signal far faster than predicted by theory, since air is not entirely transparent at 900MHz. High altitudes (where the air is thinner) will help, with the vacuum of space being near-perfect.
- **Curvature of the Earth** will eventually factor in at extremely long ranges; UHF is not reflected by the ionosphere (unlike HF which can bounce all the way around the world). This means that line-of-sight is required for best results, and at extreme ranges an increase in altitude will be required to compensate.

The final read range obtained by this system will be announced during the presentation. According to the Radar Range Equation (square-root relationships with power and antenna gain) and comparing to the retail equipment (30dBm into 6dBi of antenna == 30 feet range), our results can be predicted. We used 48.5dBm (70W) of RF into 13dBi of antenna for a power gain of 18.5dBm, an antenna gain increase of 7dBi, and an expected range increase of (18.5+7)/2 = 12.75dB (all compared to the reference retail reader). Applying our reference standard of 30 feet (and naively assuming all other things to be equal) this gives us a predicted final read range of 565 feet; you'll have to attend the presentation to find out how it turned out in real life!

Range Predictions

Given that the radar range equation holds true for Gen2, we can make some predictions about the read range capabilities of systems far bigger than the one we have built.

First, let us consider what could be assembled at "reasonable cost" and operated within the confines of amateur radio rules. Legal-limit power amplifiers are rare and expensive at UHF frequencies, but they can be built using modern parts without too much difficulty. Generally, large power amplifiers (like the one in this system) break apart an input signal into several parts, each of which is amplified separately then recombined. In this way, many small amplifiers can be used to build a single very large amplifier

at significantly reduced cost. Large antennas to handle the power are also available; http://bit.ly/dx2PmD is a suitable loop yagi that can be stacked into a 2x2 array for power handling of 2000 watts overall and gain of 26dBi. The entire combination of power amp and antenna arrays can be assembled for less than $5,000 with a predicted read range of 12,000 feet – a little over 2 miles.

Next we consider military systems. The US Navy (and several other countries) use a radar system called AN/SPS-49. This system operates on the 851-942MHz band, supplying 280 kilowatts of peak power into a parabolic dish that is 24 feet wide by 14 feet high (approximately 35dBi at 900MHz) – applying the radar range equation as before gives a predicted read range of 80 miles for this system.

Finally, we must consider the theoretical limit for such a system. The largest parabolic dish in the world is the 300-meter Arecibo radio observatory; at 900MHz this dish has an effective gain of around 70dBi. Applying a legal-limit amateur radio transmitter (as is sometimes allowed) of 1500 watts to this dish gives a read range of around 317 miles – well into the range of low-earth orbit.

In reality there are several factors which limit the read range to far less than these maximums, and one of the most fundamental may lie in Gen2 itself. There are strict timing requirements placed on both the reader and the tag, with both sides abandoning communication if timeouts are reached. Ironically, this timing restriction may be the ultimate self-imposed limit on Gen2 read range – a 10-mile read range (for a 20 mile round trip) takes about 100 microseconds, so we still believe that reading RFID tags from more than a mile away is entirely possible.

Impact on Personal Privacy

In order to consider the effect that our research has on personal privacy, we made several assumptions:

- EPC Gen2 tags can be read from at least 500 feet.
- EPC Gen2 tags are ubiquitous, found in product labels and identity documents.
- An attacker only has access to a system similar to ours, **not** the systems described above.

Given these assumptions (which we feel are reasonable), we created a list of scenarios to illustrate how this technology can be abused. This list quickly grew beyond anything that could be presented in a paper; we present only our top 10. To be clear, these are not theoretical attacks that could be achieved if the technology were advanced; these are instead attacks that are **entirely viable with the equipment we have assembled for less than $1000** and nothing more.

We assume a read range of 500ft from a vehicle-mounted solution, an angular resolution of 15 degrees (the beamwidth of our antennas), and EPC Gen2 tags in high-valued items at stores and standard-issue identity documents in all of the following scenarios.

10: Targetted burglaries

Given the prevalence of Gen2 in identity documents in many locales, it becomes possible to also detect people (by the nature of their attachment to ID). A two-part attack becomes possible:

- The attacker sweeps an affluent neighbourhood late at night looking for Gen2 identities. He plots their location on a map, and uses these to determine the homes of people carrying Gen2-based documents.
- The attacker returns on successive nights looking for the same tags. When he notices that a tag is missing, he knows that the tag corresponds to a drivers license which corresponds to a person. If the tag isn't there then the owner of the tag isn't there either, and it is likely safe to break in.

9: Shipping chains

Gen2 tags are commonly used to label inventory, both in bulk (containers) and small-scale (UPC). A long-range tag reader can also function as a long-range tag **writer** and a long-range Gen2 **sniffer**. This allows the attacker to sniff the unlock and kill codes for the tags used to track inventory, and then reprogram them. He may interfere with many levels of the supply chain in many different ways; introducing duplicates, changing tags, or simply disabling all tags from very long range. The author is not in a position to speculate as to the consequences of such actions, but would expect the result to be significant given the sheer level of Gen2 deployment at all stages of the supply chain.

8: Targeted terrorism

Gen2 is relatively common in identity documents such as Enhanced Drivers License and the US Passport Card. Different issuers of Gen2 tags (such as different states) use different prefixes for their tag ID numbers allowing (for example) a group of Americans to be identified from long range, assuming they are carrying their standard identity documents. Terrorist acts can then be targetted so as to affect maximum damage upon US citizens, as identified by their drivers licenses.

7: Spot the Tourist

Tourists are commonly targeted by muggers since they tend to carry large amounts of currency and other valuables. Given that a Gen2-based identity document identifies the state of residence of its owner, it becomes possible to identify people from specific states and hence find tourists to mug.

6: Big Spenders

Many retail chains (such as Walmart) use Gen2 to tag high-value items, both for stock control and for security. If the tags are not properly disabled at the till (which can be easily arranged by the attacker), he can identify shoppers leaving the store who have high-value goods they have just purchased. If he wishes, the attacker can tour the store with a mobile reader beforehand to find the ID numbers of specific products he wishes to target; when he sees a shopper leaving with his chosen tags (or other high-value tags), he follows the person home and obtains the goods however he chooses.

5: Retail havoc

Stores use Gen2 for stock control as well as security, conducting inventory by sweeping the shelves with a mobile reader. If an attacker can sniff the unlock and kill codes from an in-store reader (which is possible with our equipment) he can reprogram or destroy tags on goods as he sees fit, tricking the in-store computers into taking any action he wishes based on a non-existant excess or shortage.

4: 4th Amendment Hell

A read range of 500+ feet makes it possible to scan for Gen2 tags in the majority of a typical urban block with a single pass from the main street. While technically dangerous to do so (exposing the public to high levels of RF energy), such a search could potentially find people (from their ID), stolen goods (from their labels), or any other item that can be tagged with a 2” x 2” adhesive label. It is technically feasible to scan an entire city for a credit-card sized RFID tag in a single day with only a handful of mobile stations.

3: Ultimate Stag Prank

Gen2 tags can easily be purchased in bulk; for $100 on eBay we bought 1,500 to hand out at Blackhat. If someone knew in advance that a vehicle would soon be crossing the US border (such as for a vacation or business trip), a bulk order of tags can be pre-programmed with ID numbers from known EDL and PASS ranges. These tags can then be hidden around the vehicle before it approaches the readers at the border; once again I'm not in a position to speculate on the results but I would expect the border guards to be very curious why the mule has a thousand passports in his trunk.

2: Sniffing Underwear

Gen2 is increasingly being used to tag articles of clothing, often sewn into the garments themselves. It is relatively easy to walk around a store with a mobile Gen2 reader and catalogue which tags correspond to which articles of clothing. If the tags identify specific articles of clothing in sufficient detail to satisfy a major international corporation, then they also provide sufficient information for a potential stalker to...I don't really want to think about what.

1: Mall Surveillance

This “attack” deserves the number 1 slot for one simple reason – I believe that it could be turned into an entirely viable business plan that's legal in a majority of US states.

Install a box just inside each of the doors to a large mall, containing a low-power Gen2 reader as well as high-power readers for every other type of RFID tag imaginable (credit cards, passports, access cards, etc). As shoppers enter the doors and are forced to walk within range of the readers, all available RFID information is read and correlated together. Any Gen2 tags (such as a drivers license) can then be used to track the shopper as they walk around the mall; just a handful of readers in a large shopping mall and you can track the entire mall population in realtime.

The resulting data can include:

- Name
- Credit card details (card numbers, expiry date, number of cards found, etc)
- Home state
- Route taken through the mall
- Any pauses in movement, such as to look in a window.
- Details of purchases made
- Corresponding details for other co-operating malls
- Additional information (such as home address) from co-operating stores

Obtaining data on shoppers in such granular detail would be of significant value to marketers and other data miners; it all becomes possible because of Gen2's long-range nature and the fact that it is currently employed to provide a unique identifier for a person.

Ironically, the defense against all of these attacks is both very simple and widely supported (by civil rights groups and industry groups alike): Remove RFID tags from identity documents, and require companies to disable tags when products leave the store. Easy, huh?