Behind the bars

This is actually not about me getting at the bars in legal terms but it is something pretty interesting and important that could get people at the bars.
It is about the treatment of digital money in supermarkets all over Germany and other countries that make use of the technology described in the following.

Refund Systems

To those who are not from Germany or an European country it is probably not known that we have a pretty big infrastructure of refund systems. Here in Germany bottles and cans containing liquids with bubbles (sparkling water, soda pop) or alcohol have to be returned to the store when empty. To make you do that you pay 0.25 Euro more on the price of your beverages and get that money back when you return the empty bottles/cans.
Even before these new rules were released we had a lot of those cash refund systems for empty glass/plastic bottles (like water, beer, soda pop). You can return the bottles you have bought almost all over the country. In big supermarkets they have people sitting there and taking your bottles back giving you the money for it. In smaller supermarkets this is not really paying off, since you have to pay one more person for doing that work. That is where companies like T0MRA and PR0KENT come into play. They have developed big machines taking in the bottles and using infrared-vision with up to 40 pictures a second to recognise the type of bottle you inserted.

This is one of those machines serving you at European supermarkets.

Where does the money go?

The interesting question is how you get your money back. The T0MRA-600 and adequate machines do not give you any money but a receipt with a bar code number on it. You take that little slip to the cashier and they will treat it as cash for your regular shopping. They scan the code and rip it apart or sign it and then push it on a nail.
So the first thought is about the bar code. What dose the number look like? Does it make sense at all?

This is the barcode taken from a T0MRA at a local store.

As you can see you might need a little fresh up course on your EAN-13 knowledge.
EAN-13 is the typical barcode used in the European countries (similar to UPC in America). It has 13 digits of which the last is a check-sum digit. This is just a check for the hardware to make sure the code was recognised correctly. This check is done by the hardware of the barcode scanner (so no chance for developing our own checks).
The first 3 digits are the country code. Here it is the reserved code 980 standing refund systems. After that we would have the code for the company in that country and then the number of the product.
As we can see in our case we have the next 4 digits an increasing number and then the value of this receipt.

Refund-System-Security?

The number on each receipt is definitely unique for at least 1,000 customers (because of the increasing number). But it is stored and compared to a database when you try to check out at the cashier?
That is a pretty tough question and it is not easy to answer unless you give it a try. But we gave it a try with the least amount of risk there could be. This is the way to do it:
You go to a supermarket return an empty bottle and walk out with your receipt, hop in the car, drive

to the next supermarket of a different company and buy a candy bar paying with your receipt. If does not work you just say sorry and explain that you probably got that receipt from another supermarket (where is problem?). But I would not be writing this if I had to make up excuses. It worked.

Different supermarket similar receipts.

As you can see in the sample above the cash systems probably only check the country code (980) and then return the amount of money written on the receipt. It would probably be far to expensive to integrate these refund machines into every cashing system on the market.
To the pessimistic it could still be obvious that all the refund systems are connected to a big database over the internet and so I was able to get my money at the other store.

Proof of concept

After getting this far it was clear that the last step had to be done as well. And the last step was to really forge a receipt and try it out in real life.
On the back of the receipts you can see the emblems of the company of the refund machine (probably to make it hard for you without the right paper). But where to get that paper?
The machines use a special thermo print paper. It is so special that you can buy it at almost every store carrying office supplies (like STAPLES).
With a decent scanner you can scan the back side of the receipts, polish it up a little (e.g. using mspaint) and print it right onto your custom paper from STAPLES. That is a little tricky since the paper is pretty thin and not suited for a regular ink jet printer. I just used some tape to pin it to a regular size paper and then print it. Since you will cut off the parts where you taped the paper make sure it is long enough. Since we have no thermo printer you also have to let the paper dry a little longer and experiment a little with the way the colour comes out.

To print the other side you need to scan it again and customize it in you graphics program of choice. The bar code needs to be replaced (unless you just want to multiply this one receipt). Creating the bar code is the least problem since we know every single digit and Google knows the rest (there are even java applets for generating EAN-13 from web pages).

I played it safe

After I had faked my receipt I went to the store and asked the people there if I could try something for a research project of my school. I had to wait quite some time until I was allowed to let them scan my receipt (and I even had to buy something). You can see that I only replaced the bar code in this test. It is an old receipt but with a barcode worth 99.99 Euro.

Input

Output

Any way to protection, Mr. T0MRA?

As you know it is always good to inform the people creating these machines about their problem. So I wanted to report what I had discovered and set up a letter to the company.
If you know some German it is definetly better reading the three letters sent between T0MRA and me in German. They are found here.
My letter explained the way you could forge those receipts and I asked whether there was any way to connect the cashier and the T-600 or any other of their products so forging receipts would not be possible anymore.
The answer was:

"... Do completely explain why you sent this mail and tell us your complete postal address. ... If you have contacted us on behalf of a company then tell us their name as well..."

We don't care for our customers at least not for you!

Well I wrote back telling them that I was not working for any company, that I was a student and that

if they wanted to I would be happy to help them developing system for synchronising the cash desks and their machines.
After that mail I never heard of them again. And now almost three years later nothing has changed (as far as I can see).
To me this means that a company like that does not really care for the security of their customers (the supermarkets).

I have written to other people concerning security issues in their applications. It looks like the companies of a certain size (> 20 employees) don't care about others wanting to help them.