RF-ID and Smart-Labels: Myth, Technology and Attacks

DefCon 2004

July 30 - August 1, Alexis Park, Las Vegas, NV

Lukas Grunwald

DefCon 2004

Agenda

What is RF-ID ?

- What is RF-ID and what are Smart-Labels
- Risks and dangers with them
- Fun with them, how to protect your privacy
- Attacks against Smart-Label Systems, RF-ID Systems
- Demonstration of RF-ID Tags and RF-DUMP in practical use
- The RSA-Blocker-Tag fake
- The Metro Future Store

RF-ID

RF-ID (Radio Frequency Identification) is a mechanism to get an identification remotely from:

- your remote-control for your garage
- an access control-system for a room
- a cage in a factory
- an electronic product code attached to a wrapped item in the supermarket

Frequencies

RF-ID (Radio Frequency Identification) operates globally on different frequencies, the most common systems are using the ISM (Industrial Science Medical) Bands:

6765 - 6795 kHz	40,66 - 40,7 MHz	24 - 24,25 GHz
13553 - 13567 kHz	433,05 - 434,79 MHz	61 - 61,5 GHz
26957 - 27283 kHz	2400 - 2500 MHz	122 - 123 GHz

Smart Labels - EPC

Smart-Labels are a special form of an RF-ID application. The tags look like normal product tags, but inside is an antenna and a small microchip. The tags have a Serial Number and an EEPROM that can store information like the EPC (Electronic Product Code), an international unique code from the manufacturer. Now the labels have mobile communication capabilities.

EPC Type 1			
01	0000A66	00016F	000169DCD
Header	EPC Manager	Object Class	Serial Number
8 Bit	24 Bit	24 Bit	36 Bit

The ISO-Standard Smart-Labels operate on the ISM Frequency 13.56 MHz

Smart-Label - Variants

Some of the well-known cheap Smart-Labels you´ll find today and tomorrow in some consumer-products are:

ISO 15693	Tag-it ISO, My-d, I-Code SLI, LRI512, TempSense
ISO 14443 A	Mifare Standard(1,2), Mifare UltraLight(1,2)
ISO 14443 B	SR176(1,2)
Tag-it®	
I-Code®	

Smart-Label - Features

What the Tags have in common:

- have no battery, and consume the power to operate from the RF-ID reader-field
- store the information in clear-text on the EEPROM
- have memory pages
- do not have read-protection
- some have special write protection
- Tag-Serial-Number is fixed, user-data is flexible
- support up to 1000 write cycles

Smart-Labels

The Labels are used by manufacturers and delivery companies to optimize their supply chain:

- easy integration at the production plant
- tracking of boxes and goods
- easy sorting of boxes and packets
- just-in-time production
- tracking of the max. temperature for sensitive good (medicine, reefer cargo)

Data-Center vs Tag

- The information about a product can be stored in an central database, and only the native serial number of a Tag is used, or all information can stored on the EEPROM directly in the labels.
- In the field we often find a combination of both approaches where some information is stored in the label, and some is held in a central database.

Smart-Labels in the US

- FDA Guidance Mass
  - 2005 Mass serialization of some packages, cases & pallets likely to be counterfeit.
  - 2005 Use of RFID by some manufacturers, large wholesalers and some chain drug stores and hospitals.
  - 2006 Use of RFID by most manufacturers, wholesalers, chain drug stores, hospitals and some small retailers.
  - 2007 Use of RFID by all manufacturers, wholesalers, chain drug stores, hospitals and most small retailers.

Source: Robin Koh, MIT Auto-ID Labs

Smart-Labels in US Part II

- Florida
  - July 2003 Pedigree for Top 30 drugs
  - July 2006 Pedigree for all drugs
- Walmart
  - June 2004 All Class2 drugs

Source: Robin Koh, MIT Auto-ID Labs

Smart-Labels in Europe

- The Gilette Company
  - up to 35% loss of their products from the plant to the shelf in the store
  - massive problem with shoplifting, small and in-expensive products like razor blades
  - most products with RF-ID Tag inside of the product.
- Metro Future Store
  - extensive use of RF-ID and other new technologies
  - more later ..

Smart-Labels in Europe

- Main Library Vienna
  - Use of more then 344000 Tags on books, DVDs, CD-ROMs etc ...
  - Stores directly on the label:
    - ISBN (International Standard Book Number)
    - Author
    - Title
    - Last date of rent
- The EU Government
  - Electronic Passport with RF-ID Chip
  - Chip stores your ID-Number and Biometric Data

Not only in Food

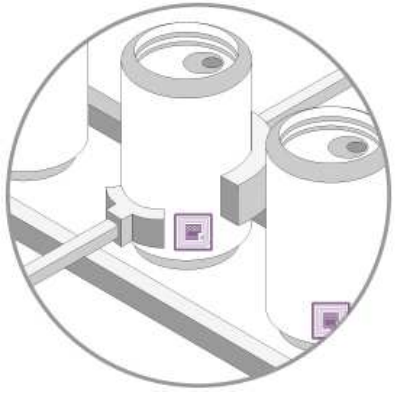
- Some Cloth Companies also use RF-ID Tags
  - Gap Inc. in the US
  - Kaufhof in Germany
  - Benetton from Italy
- There are also Tags and pilot project where chips are woven directly into the fabric.

POS Benefits

Benefits of Smart-Labels at the Point of Sale:

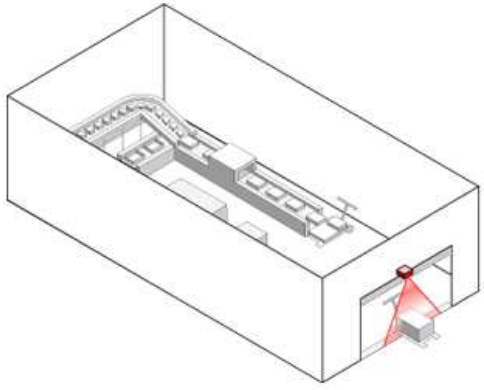
- auto inventory
- detect misplaced product at the shelf
- alerting the clerk to replace expired goods
- track the behavior of the customer in the shop
- auto-checkout for the customer, only put the goods in your shopping bag
- the register is an RF-ID Gate, you only need to use your credit-card or have your RF-ID customer card with you to make a quick check out

Brave new Supply Chain 1



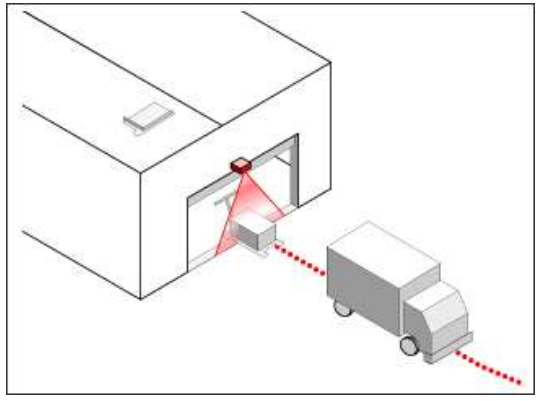
- At production time, the RF-ID Smart label is placed on the product

Brave new Supply Chain 2



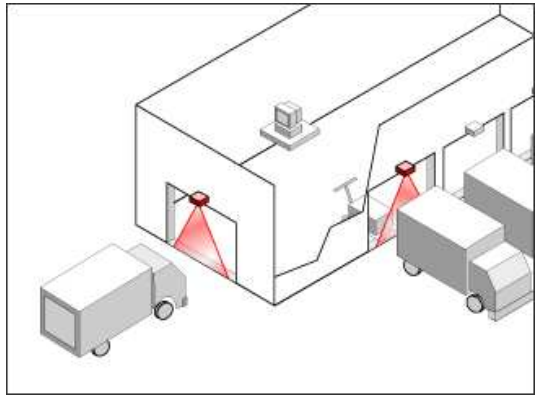
- Each product is registered inside its package when leaving the factory
- EPC is written here to the ID-Tags

Brave new Supply Chain 3



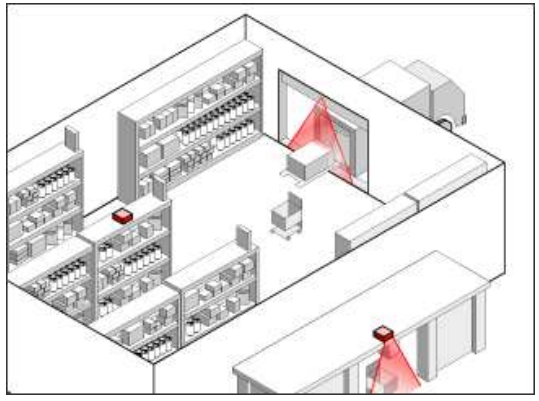
- If a customer of reseller orders the product, the palettes are tracked at delivery

Brave new Supply Chain 4



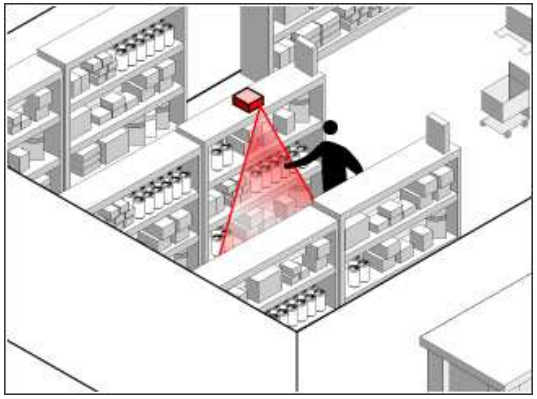
- At the reseller site, the new goods are registered upon arrival
- Temperature and expiration date can be checked at delivery time

Brave new Supply Chain 5



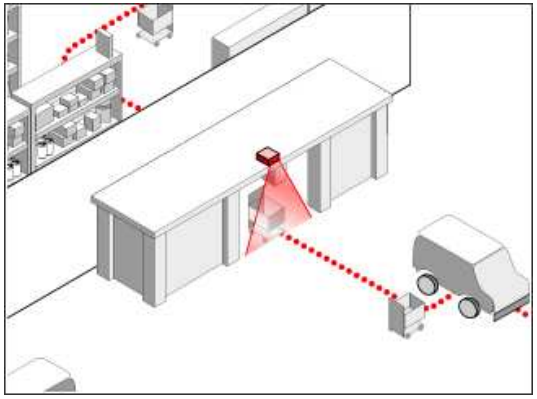
- The pallet arrives at the store, all products entering the store are registered by the entry gate of the store

Brave new Supply Chain 6



- In the store the customer take a retail-package, the RF-ID reader in the shelf detects this
- If the shelf runs out of products or detects a false returned product it can escalate this to the clerk in the shop

Brave new Supply Chain 7



- The customer leaves the store, the register reads the RF-ID from inside the customer's shopping-bag
- Fast self-checkout and shop-lifting prevention at the same time

Smart White Goods

Benefits for the customer should be the intelligence of the domestic appliances.

- Intelligent fridge
  - Auto-Inventory
  - Management of expiration of goods
- Intelligent washing machine
  - Automatic choice of correct program
  - Detecting red socks in between white undies

Myths and Facts about RF-ID

- Myth:

RF-ID´s have the size of a pin and can be embedded into every product.

- Fact:

This is not true, the electro-magnetic fields have problems with metal and other shielding material. You also need an antenna to connect the RF-ID Chip to the field, the antenna has some size.

Myths and Facts about RFID

- Myth:

RF-ID Chips can be read from a huge distance.

- Fact:

This is not true, you must be in a field to power the Chip via the antenna, the maximum distance within a huge gate are 10 meters.

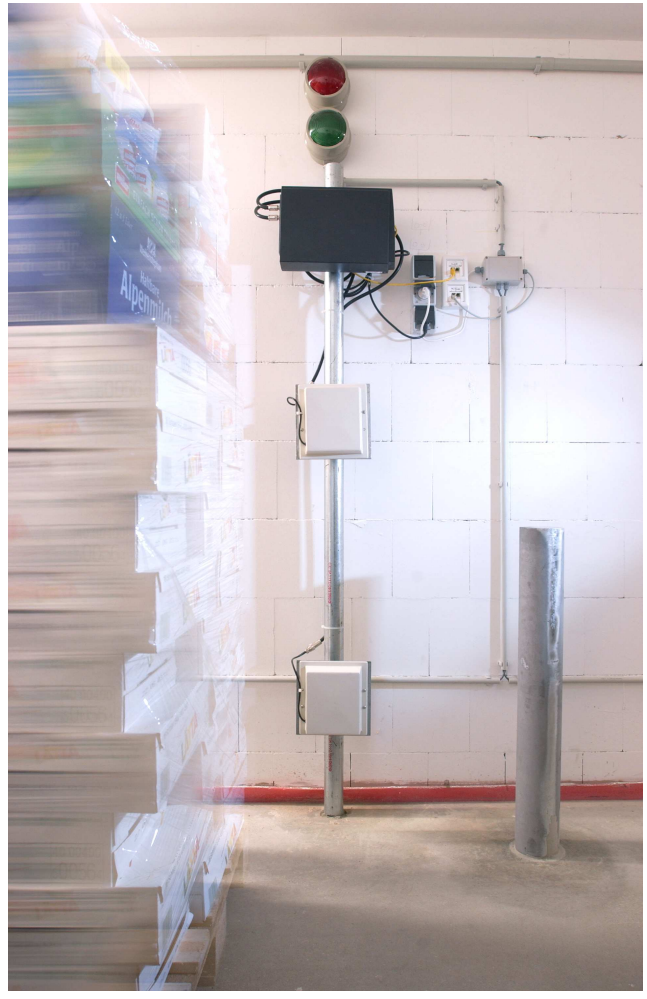
Public Information

RF-ID Tags can be read by everyone! You need:

- RF-ID Reader, we use the Multi-Tag Reader from ACG Germany
- an antenna or a gate to build the field
- Tags
- A PC oder Laptop to process the information from the reader
- Our tool to process the information

RF-ID Gate

Gates can be installed at any place: At the entrance and exit doors, the stock etc...



ISO 15693 Tags

- Each tag has an unique identifier (UID)
- UID is needed for anti-collision algorithm if more then one tag is in the field
- UID is factory programmed and can't be changed
- The Tag Memory is partitioned into two blocks
  - Administrative Block that contains
    - unique identifier (UID)
    - application family identifier (AFI)
    - data storage format identifier (DSFID)
- User Data
  - stores up to 128 Byte of User Data persistent

UID of the ISO 15693 Tag

- Coding of the Unique Identifier

Byte							
7	6	5	4	3	2	1	0
E0h	MFR	Serial number					

MFR of the ISO 15693 Tag

- Coding of the Manufacturer ID

MFR-Code	Company
02h	ST Microelectronics
04h	Phillips Semiconductors
05h	Infineon Technologies AG
07h	Texas Instrument
16h	EM Microelectronic-Marin SA

Memory organization

- Memory Organization of the ISO 15693 Tag

page	Byte			
	0	1	2	3
Administrative block				
00h	User data block			
...	...			
3fh	User data block			

RF-DUMP

- a small tool to read and write ISO Tags and Smart-Labels by Boris Wolf and Lukas Grunwald
- supports and detects nearly all Smart-Labels
- requires an ACG Compact-Flash RF-ID Reader
- runs on PDA and notebook
- Free-Software (GPL) http://www.rf-dump.org

The RSA Blocker-Tag Part 1

- At the CeBIT 2004 RSA Security announced and demonstrated a "blocker-tag": This Tag was said to block any requests.
- They presented a demo with their Tag and a box of drugs, and a paper-bag with the Blocker-Tag.
- This Tag should send all possible UID's to keep the customer's privacy when leaving a drugstore.

Let's verify the information with our new tool!

The RSA Blocker-Tag Part 2

- All pseudo-privacy is done by the fake software.
- If both Tags are in the RF-ID Field, the RSA Demo-Application claims "BLOCKED".
- In fact the customer information is still accessible by an attacker or a spy.

Attacks against Smart-Labels

- Most Smart-Labels are not write protected
- The UID and Administrative block can’t store the EPC
- EPC is stored in the User Data Area
- Meta-Data like "best-before" are also stored in the User Data Area
- It’s only a matter of time until everybody will wear at least one RF-ID Tag

Privacy Problems

- Gates can by installed anywhere
- Competitors can read what type of undies you wear, and what else you have in your shopping bag
- Big Brother can read what type of Books you read
- Together with a passport or customer-card with RF-ID Chip this technology is an even bigger risk
- The customer is traceable for everyone

Environmental Pollution

- If every retail packet has a RF-ID Chip, there will be a sizable environmental pollution issue
- The transponder or tag itself contains some harmful substances
- Non-ionizing radiation, there are some voices that say it could be unhealthy

Technology Problems

- Dependency on a new technology introduces new risks
- Attacks to the RF-ID infrastructure can push companies out of business
- New possible break for terrorist attacks and new critical infrastructure

Real-Life Cookie

- Like on Web-Sites you can put a real-life cookie on someone who wears a cloth with Smart-Label or carries an item with a Tag.
  - Every time he passes your Gate or RF-ID Field e.g. in front of your shop window you increment it by one
  - The next time you get your credit-card number, you can write his tag with a clear id, you know who was looking at you shop window
  - You can also check if the customer takes a product out of the shelf and puts it back, so if he is unclear, you can make an instant discount only for him in 10 sec.

The Metro Future-Store

The Metro Future-Store

- Initiated by the Metro Corporation and a several technology partners
- First store using RF-ID technology at some customer shelves
- Uses RF-ID Technology for age-control for X-Rated movies
- uses RF-ID Technology for every palette in stock
- Puts ISO-Tags also in customer cards.
- After immense protest from privacy organizations offered a RF-ID De-activator
- Nice homepage http://www.future-store.org

The Metro Future-Store

The Metro Future-Store

- Customer can use a PSA (Personal Shopping Assistant) and can check every product he puts in his shopping bag
- Customer can also use a self-checkout
- Customer is the guinea pig for the new technology
- Perfect area for our first field test of RF-Dump

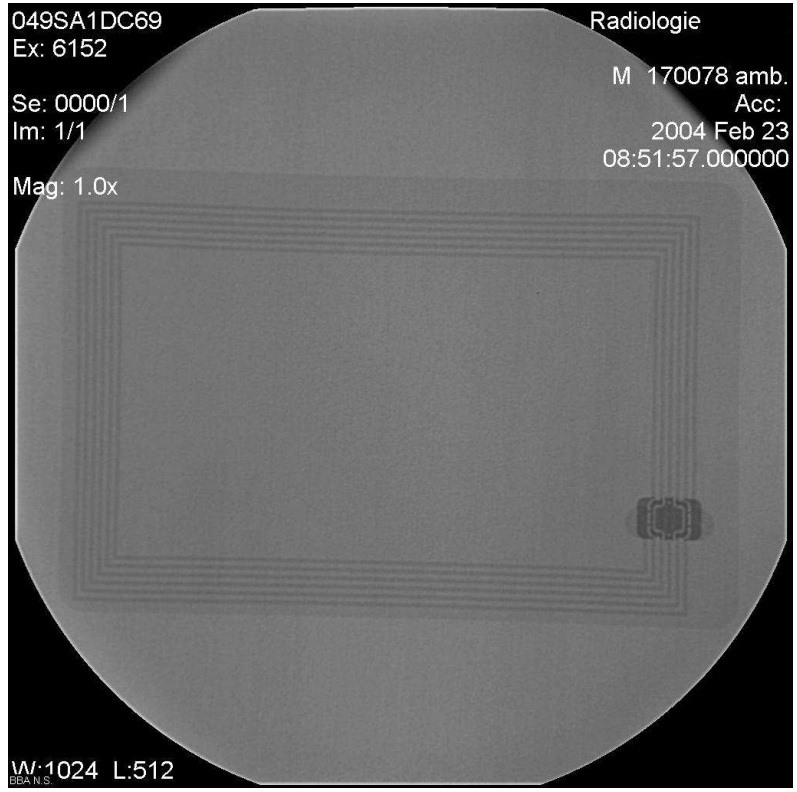
The Future-Card

- Customer-Card from the Metro Shop

Source: http://www.spychips.com/metro/scandal-payback.html

The Future-Card

- X-Ray proves there is a hidden RF-ID Tag inside the customer card



Source: http://www.spychips.com/metro/scandal-payback.html

Future-Store Testfield

The RFID-Deactivator

- After the checkout Metro offers a "RFID-Deactivator" to the customer
- In fact, it overwrites the User-Data Area with Zeros
- Tag can be rewritten after the De-Activation
- Serial-ID and Administrative Block can’t be erased
- At the Exit-Gate the Tag can be instantly filled with other information
- To use the Deactivator all User-Data Areas MUST be writable in the shop, which offers a lot of options for new attacks and fun in the shop.

Future-Store Testfield

Chaos in the Future-Store

- You can convert the EPC from cream cheese into shampoo, the store computer believes your cream cheese is misplaced in this shelf
- Put the cream cheese after converting in the shampoo shelf
- Make some X-Rated movies G-Rated, now Kid's can buy them with the Self-Checkout
- Convert your favored new DVD into the one on sale for 5 Euro

Fun with the EAS

1. The Electronic Article Surveillance (EAS) Gate at the Entrance checks also if you don't pay for your DVD via RF-ID.
2. To deactivate this Security System, get a cheap Tag for 50 cents, copy the EPC from a DVD that is in the shelf
3. Transfer it to you own tag
4. Stick the Tag under the Gate
5. The Gates goes on alert
6. Some clerk will come and check, after 5 minutes of permanent alarming he will switch the EAS Gate off

Further Attacks

- The most software is written without security in mind, at least supply chain software, it could be possible to exploit it via a manipulated data field in the User-Data of an RF-ID Tag
- Some registers make an instant reboot after reading the RF-ID Tag with manipulated field
- If you shield the field, no EAS or RF-ID System can possibly read a tag, some aluminum foil works fine

For Your Privacy

- DO NOT buy any product with a credit card and do not use any customer cards
- If you MUST use a credit card, add entropy to your customer record
- there are some interesting pages e.g:
  - http://www.stop-rfid.org
  - http://www.boycottgillette.com
  - http://www.boycottbenetton.org
  - http://www.spychips.com

Risks for the Companies

- Whole new area of shop-lifting
- Chaos and attacks are possible
- Customers can change the EPC and no-one will detect it when using self-checkout
- Attacks can also be used on medical drugs and age-restricted material
- Attackers need only a publicly available RF-ID Reader/Writer

That's it..

THANK YOU !

Questions ?

email: lukas@übergeek.de