Jemandem einen Strich auf die Rechnung machen…

Phenoelit

24C3, 2007, Berlin, Germany

Agenda

- Quick intro into barcodes
- Encoding and decoding
- Scanners
- Simple tricks
- Backend attacks
- Selected samples decoded
- Unsolved cases and an invitation
- Principles of secure barcode use

Disclaimer

- Dear audience: This talk covers observations made of widely used and well documented systems
  - Trying anything against them may be considered a criminal offense
  - I'm not encouraging you to do that
- Dear law enforcement: you can keep your hacker-tool-laws under the table
  - We only need brains and printers for that
  - Systems 101 + Barcode 101 = ***202c***odes ☺
  - Yes, that's you, the one with the Internet printout and attached translation

The History of Barcodes

- Developed 1948 by Silver and Woodland at the Drexel Institute of Technology
- First usage attempt was the Association of American Railroad to identify the cars in 1950.
  - It took until 1967 to develop the system.
  - It took seven years to label 95% of the cars.
  - It never worked.
- 1966, the National Association of Food Chains required equipment to speed up the checkout process
- 1969, the same NAFC requested an industry standard, which became Universal Grocery Product Identification Code (later: UPC) in 1970.
- 1981, the US Department of Defense required Code 39 to label all products sold to the military.

1D Symbologies

Code 39	
UPC-A to UPC-E	
EAN8	
EAN13 and EAN13 with supplement	
RSS-14	
CODABAR	

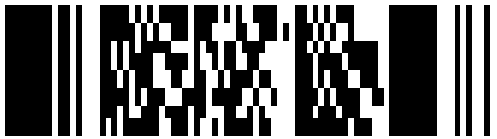
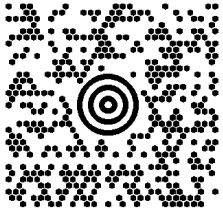
1D Symbologies

Interleaved 2 of 5	
Discrete 2 of 5	
Code 93	
Code 128	
EAN/UCC 128	

1D Symbologies

Postnet	
BPO 4 State Code	

2D Symbologies

PDF417	
Data Matrix	
MAXICODE	
AZTEC CODE	

Barcode Decoding

- Barcode scanners
  - 1D hand scanners are cheap
  - All scanners can be configured to output the barcode type using a type character when decoding
  - Don’t get a better scanner that what you plan to attack (more on this later)
  - 2D scanners are still expensive
- Decoding software
  - Some is free
  - Others can be cracked easily
  - I’m lazy and have chosen the capitalist way: Omniplanar SwiftDecoder

Barcode Generation

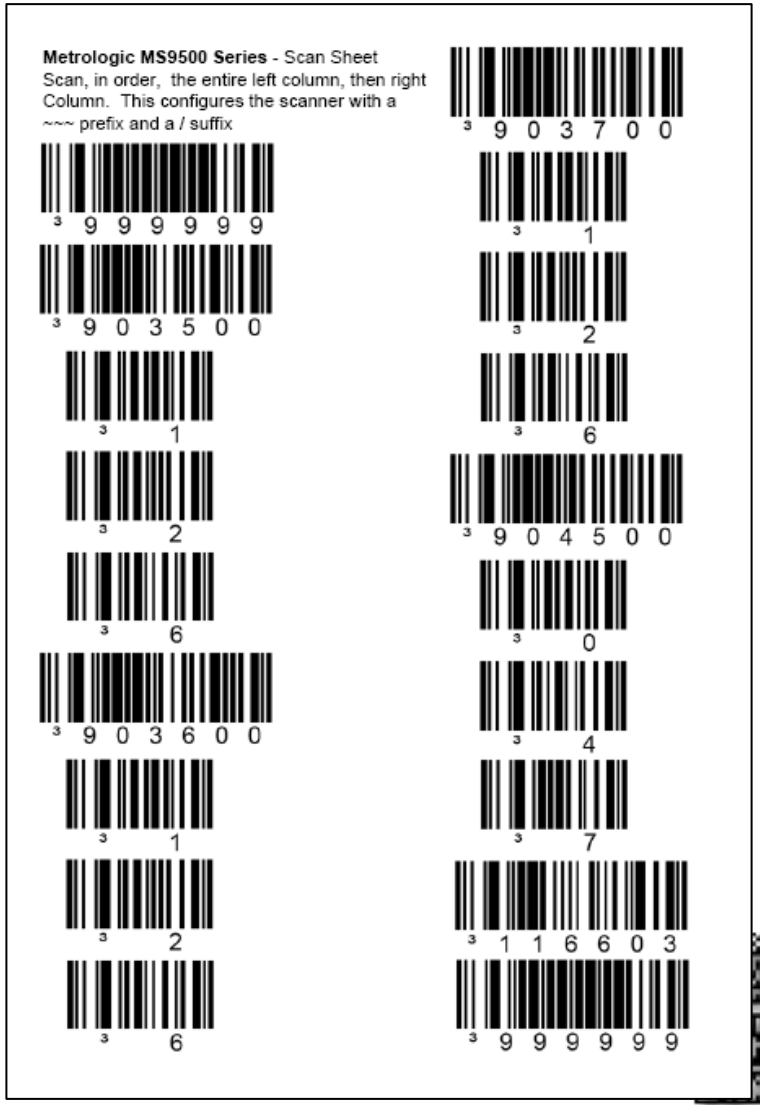
- There is a lot of barcode generation software out there
  - Free: GNU barcode (1D only)
  - Online: ask your favorite search engine
  - Commercial: uncountable
- Writing generators is not hard
  - Usually, you have to pay for the specs
  - Most specs are below $20 US (next year that’s € 3,50)

Applications

- Barcodes are in general used for three purposes:
  - Tags and IDs
  - Data transport and virtual to physical media
  - GGU (Ganz grober Unfug)

Configuring Scanners

- Almost all scanners are configured via barcodes
  - Scan “Enter Configuration” barcode
  - Scan configuration barcodes
  - Scan “Save Configuration” barcode



Configuring Scanners

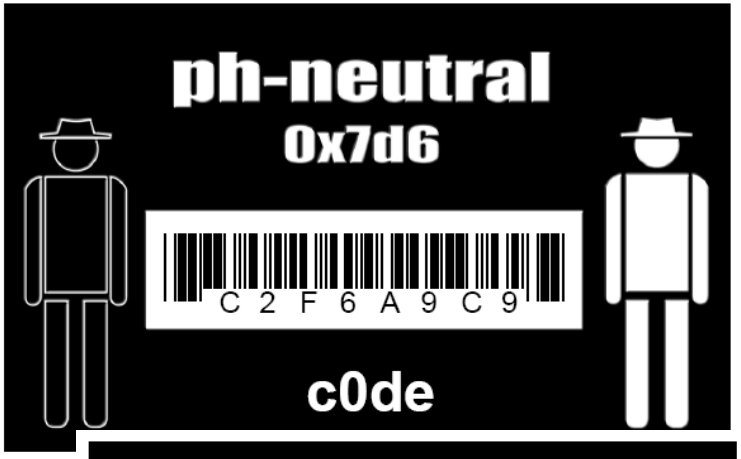
- Find out what vendor's scanner is used
- Get the configuration sheet
  - Vendor's support web page
  - Dealer's support web page
  - Just call them
- Reconfigure the scanner
  - Change supported barcode types
  - Change CRLF
  - Change character encoding
- Most scanners support special "key codes" like ESC, PageUp, PageDown, DEL, etc.
- Some scanners support **software updates** via configuration codes.

Copying Barcodes

- Often, it is sufficient to copy barcodes
  - You don’t have to decode them if you know what the code does for you
- Get a good digital camera
- Get a printer

PH-Neutral

- Barcode was used as authentication against the bar ☺
  - You could “load” money onto your badge
  - Drink without paying
- Stefan Sels successfully copied a b33r badge using his digital camera
  - It worked!



Parking

- Hotel parking garage in Dresden does not enforce correlation between entry ticket and exit ticket
  - Paper tickets with barcode
- They also have long-term parking tickets
  - They also give you one temporarily if you stay in the hotel
  - Parking for free; forever

Recycling Machines

- You feed bottles into the machine
- It counts their value
- It produces a voucher
- Get your money from the cashier using the voucher

Getting paid for drinking Beer

- There is no connection between the recycling machine and the cashier's system
  - People used to simply copy the vouchers
  - Current versions are printed on "watermarked" paper
- The vouchers use a special property of the EAN13 barcode: the leading number code
  - EAN13 codes start with the country of origin
  - Number 2 is reserved for "store internal use"

Getting paid for drinking Beer

- Leading 2:
  Store Internal
- Following 6 digits: Cash register code for “money back”
- Following 5 digits: value
- Last digit: 10 minus the sum of all digits (EAN13 checksum)

➔ Generate your own and stick it under some heavy item (sixpack)

Access Control

- Some organizations use barcodes to control physical access
- More often then expected, the access control system only verifies that the structure of the data is well formed
  - Easy test: show it your pack of cigarettes (or candy bar for non-smokers)
  - More advanced: get the number of digits and the barcode type right

De-Synchronization

- People read the number printed next to the code
- Scanners and backend systems read what is encoded on the barcode
- They don’t have to be equal

De-Synchronization

- People play this trick with you as well: The Zoo Berlin
- The barcode “says”:
  3711679,
  3711682,
  3711683…
- The barcode decodes to:
  49864088922304,
  59264988922604,
  59364988922704…

De-Synchronization: Property Tracking

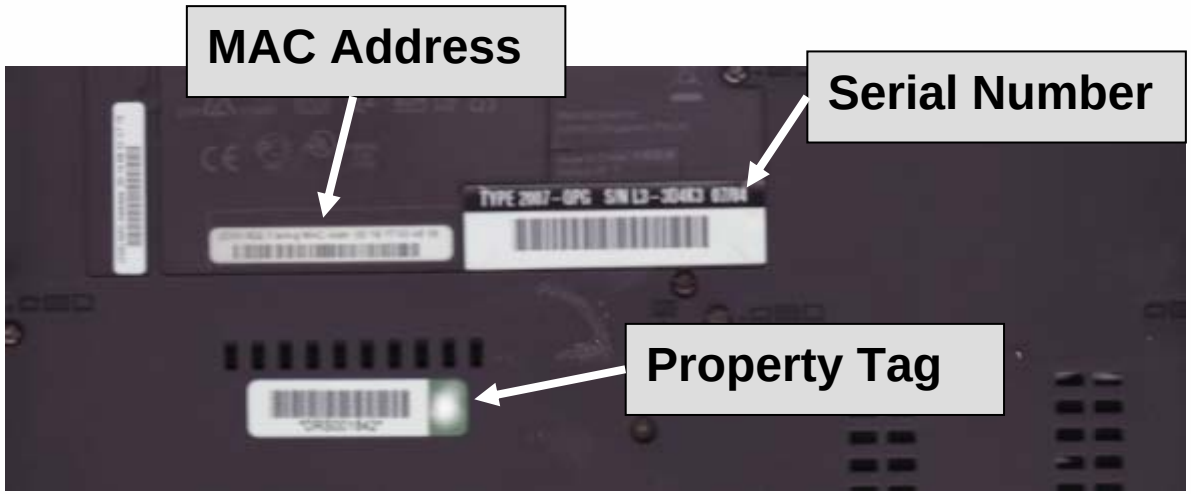
- Property must be checked in when entering the building
  - Connects your badge barcode with the property's barcode
  - Checkout works the same way

➔Replace the barcode on your badge temporarily with the barcode on the badge of the legitimate owner

  - Check out with your new property
  - Check in again without anything
  - Remove replaced barcode from your badge
  - Check out and go home

De-Synchronization: Property Tracking

- Works as well with inventory numbers (ever wanted this company laptop to be your own?)
- Works well with MAC addresses too.



Procedure is Key: Video24

- Automated DVD rental system
- Barcode member card, PIN, Biometric authentication (!!1!)
- Rental Procedure:
  - Swipe card, enter PIN, select movie, logout
  - Can be done via their Web Site
- Pickup Procedure:
  - Swipe card, get DVD from machine
- Return Procedure:
  - Swipe card, enter PIN, put DVD in machine

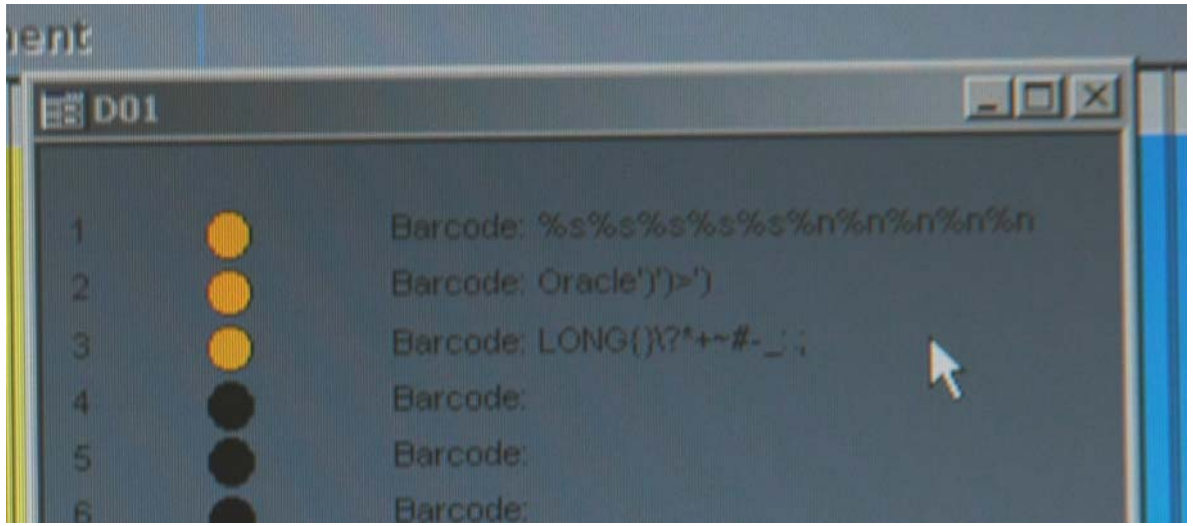
Procedure is Key: Video24

- Code 38, 5 characters on member card (CCD readers in machine?)
  - Easy to try some
  - If open order, you get a DVD
- 5 digit code on DVDs
  - Replacing a DVD with an empty one requires PIN
  - Can be verified on the Web Site beforehand
  - Not a good idea: last placement is traceable

Injections and Multi-Decoding

- Most barcode readers are left in their factory configuration
  - Even if they are not, one can reconfigure them
- The back end application will, in many cases, only expect the barcode type it is written for
  - Usually EAN13 or Interleaved 2o5
- Using Code 128, one can inject arbitrary characters as input
  - SQL Injections
  - Separation character injections
  - Format String attacks
- The newer the system, the better this works!

Injections and Multi-Decoding



QR-Codes

- Take a photo of a 2D barcode on your newspaper
- Commercial (!!!) decoder software will convert it into a HTTP hyperlink
- The software will send your mobile browser to that URL

2 WELT KOMPAKT

SO FUNKTIONIEREN DIE CODES

1. Sie brauchen eine kostenlose Software und ein Handy mit mobilem Internet. Datenpakete für mobiles Surfen gibt es schon ab monatlich 10 Euro. Sonst wird es teuer.
2. Schicken Sie eine SMS an die *22622*, Stichwort: kompakt oder tippen Sie die Web-Adresse: *mobil.welt.de/reader* in Ihr Handy.
3. Ihr Handy wird nicht unterstützt? Wählen Sie aus der Liste, die Ihnen das Programm zeigt, ein ähnliches Handy aus. Oder laden Sie die Software eines anderen Anbieters herunter: *www.activeprint.org*
www.neoreader.com
www.quickmark.com.tw
www.i-nigma.com

Unter www.jepblog.de finden Sie drei Filme, die die Codes erklären

Point and shoot
1. Handy mit Reader-Software auf den Code richten und fotografieren
2. Der QR Code (QR = quick response = schnelle Antwort) ist ein zweidimensionaler Barcode, der z.B. eine Webadresse enthalten kann.
3. Das Mobiltelefon übersetzt den Code und verbindet sich direkt mit der Website. Das Eintippen der Webadresse entfällt.

WELT KOMPAKT *INFOGRAFIK*

QR-Codes: Die Welt

Ab heute gibt es Bildergalerien

Berlin – Mit unseren QR-Codes, die Ihr Handy auf Seiten ins Internet leiten, ist WELT KOMPAKT noch technische Avantgarde. Immer mehr Zeitungen wie die Times und Sun in England ziehen nach. Heute beginnt ein neues QR-Kapitel, denn wir bringen Sie jetzt auf Bildergalerien und Fotoserien im Internet. Zum Auftakt gibt es – seien Sie uns nicht böse – die 100 schönsten Frauen des Jahres 2007. Ausgewählt von den Kollegen der Zeitschrift Maxim. Viel Vergnügen.

Wer ist die schönste Frau 2007? Jessica Alba ist auf Platz 2

Leben, Seite 25

Der Pole Marek Fiuk vor seinem Haus bei Löcknitz – er hat die Seiten gewechselt.

...h. Täglich kommen ...e polnische Schüler ...Autobus aus dem ...m nach Vorpom- ...das deutsch-pol- ...sium in Löcknitz ...a 160 polnischen ...cht. Täglich kom- ...polnischen Ärzte zu den Schichtdiensten in das Krankenhaus von Pasewalk oder die polnischen Lkws mit Lieferungen für Schwedt, wo europaweit eines der größten Zentren für erneuerbare Energien entsteht. Nun wird der Alltag eben noch normaler, als er bisher schon war.

Europa wächst zusammen: Slideshow von der Grenzöffnung

Unklarheit nach Karlsruher Jobcenter-Urteil

QR-Codes: Die Welt

- The codes actually contain a link to a “mobile blogging” company:

```
 wget http://decode.kaywa.com/1200200370325
--20:43:30--  http://decode.kaywa.com/1200200370325
           => `1200200370325'
Resolving decode.kaywa.com... 212.90.220.9
Connecting to decode.kaywa.com|212.90.220.9|:80... connected.
```

```
 wget http://decode.kaywa.com/1200200370322
--20:43:46--  http://decode.kaywa.com/1200200370322
           => `1200200370322'
Resolving decode.kaywa.com... 212.90.220.9
Connecting to decode.kaywa.com|212.90.220.9|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://www.iphone-ticker.de/2007/12/06/imatrix-
praktisch-coole-qr-code-spielerei-video/ [following]
```

QR-Codes: Injection

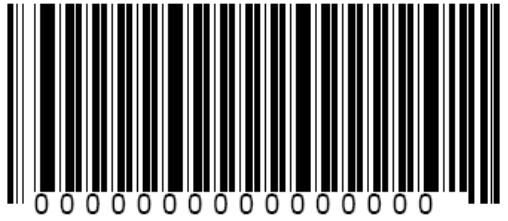
- People can print arbitrary content in newspapers: it’s called advertising
  - Most people trust their newspaper (at least the security of it, not necessarily the content)
- The browser on the mobile phone may already run
  - Active authenticated session cookies ?
  - Vulnerable Browser ?

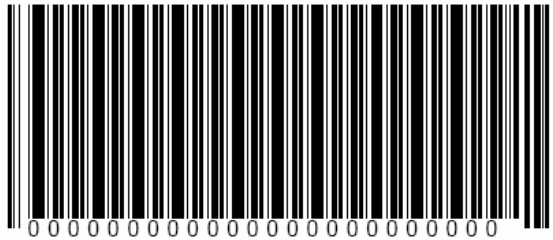
Cross Zeitung Scripting

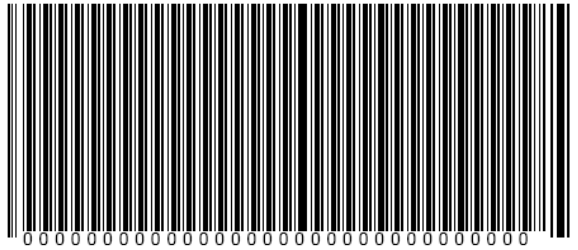
- XSS via a newspaper !!1!
- How about …
  - … a link to your control your gmail account?
  - … a link to an ICEPACK / MPACK site?
  - … a link to a binary for your mobile phone?
  - … a link to **`about:`** or **`chrome:`**?
- Thanks!
  Now we need to tell our managers to not click links in their newspaper. OMFG!

Length and Decoding

- The better 1D codes do not specify the amount of characters you can encode
- The better your printing resolution and the attacked scanner (laser preferred), the more data you can stuff into the code
- Have you ever noticed that more data than expected is a desired property for people called hackers? ☺







Barcode driven Buffer Overflows

- Yes, they happen.
- No, it is a lot less common than one may think.
- Your tool of choice: Code 128
  - Full 7-Bit ASCII character set
  - Chainable using Function Code FC4
- Warning: It’s a pain.

QR-Code Readers Again

```
.text:10006EB4 aThisApplicatio DCD 59
.text:10006EB4                 unicode 0, <This application is for use only within the >
.text:10006EB4                 unicode 0, <European Union.>

.text:10006F88 a442073952625   DCD 13
.text:10006F88                 unicode 0, <+442073952625>

.text:10006FA8 aRtspS          unicode 0, <rtsp://%S>,0

.text:10007950                 unicode 0, <212.183.137.12>

.text:100071C0                 unicode 0,
<http://ap.hpl.hp.com/resolve.php?v=1&a=g&d=>

.text:10007288                 unicode 0, <http://activeprint.lavasphere.de/
lava_key_generator/?login=HPglass&pwd=yoC9boon&sis=1&ver=0.9&imei=%S>
```

Things that didn't break ☹

Things that didn't break ☹

- They use Interleaved 2o5
- Their scanners accept almost all 1D barcodes
- Their application doesn't care at all.
- Well done IKEA!
- May be we should try again in Moscow, they seem to have a different management.

Recreation Attacks

- If we can predict the meaning of the barcode, we can create our own
- Yes, it’s that simple.

Postal Codes

- Postal services increasingly use 2D barcodes to replace stamps.
  - Automated generation
  - Automated verification
- Some use their own special barcode types
  - Less decoders are capable of dealing with them
- Most use DataMatrix
- But what exactly is verified?
  - Depends on what is in there ☺

Postal Codes: Swiss

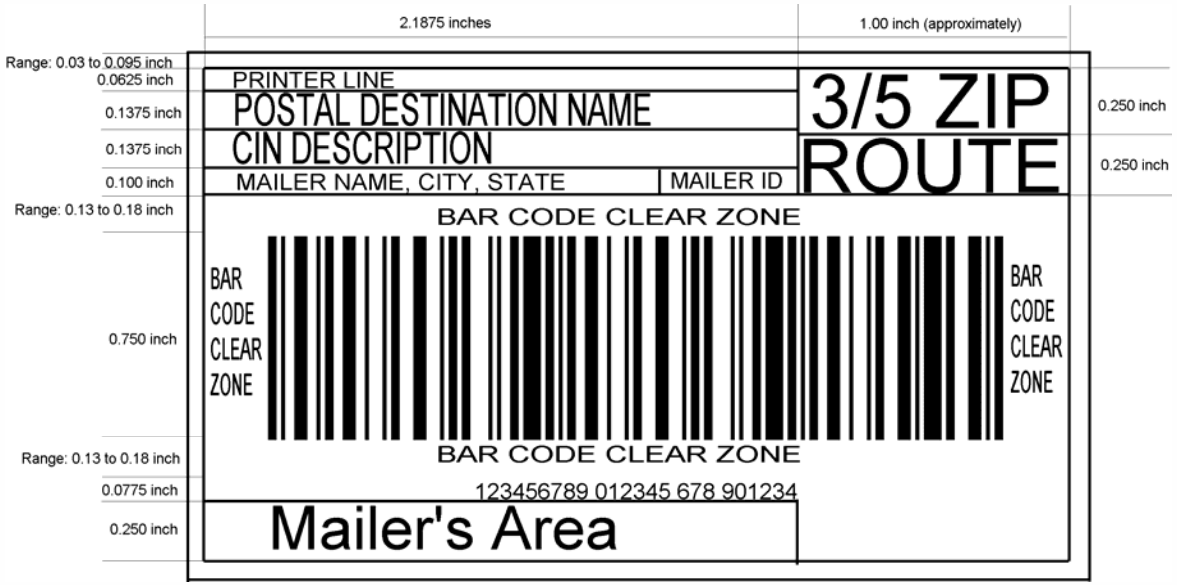
Australia Post **ASCII “00,00000000,000000000000000000000000000000”**

Interleaved 2 of 5
0100610149055028

Interleaved 2 of 5
870463835002

US Postal Service

- Labeling System called “Intelligent Mail”
  - Uses Code 128 labels
  - Specs can be found on the Internet ☺



US Postal Service

Element	Digits	Purpose and Details
ZIP Code:	1 - 5	Identifies the tray or sack's destination. For 5-digit trays in accordance with the DMM, the destination ZIP Code is the 5-digit ZIP Code. For 3-digit trays in accordance with the DMM, the destination ZIP Code is the 3-digit ZIP Code followed by two zeros.
CIN:	6 - 8	Describes the contents of the tray or sack based on the 3-digit content identifier numbers listed in the DMM. If no listing for the tray contents is found, three zeros are used.
Label Source	9	Use the value 1 for Automation Compatible, Barcoded, and Machinable Mail. Use the value 7 for all other mail. *1 and 7 are the only acceptable values.*
Mailer ID:	10 - 18	A unique, nine-digit number assigned by the Postal Service to each mailer.
Unique Identifier:	19 - 23	A unique, five-digit number for each tray or sack.
Label Type:	24	The Label Type is used as a qualifier for systems to recognize and parse the data within this barcode. The value is 8 when used with the 9-digit Mailer ID.

US Postal Service

"*To maintain uniqueness of the barcode, the data for these label types must be unique for 30 – 45 days. Mailers are asked to check with their Postal Service Marketing representative to confirm the requirement for uniqueness for a specific program.*"

US Postal Service

Pentagon Building Securi
and
Emergency Procedures Gui

Developed by the Pentagon Force Protection Agency to assist Department of employees in understanding security procedures and how to handle emerg situations.

PENTAGON POLICE DEPARTMENT

LETTER AND PARCEL BOMB RECOGNITION POINTS

- Foreign Mail, Air Mail and Special Delivery
- Restrictive Markings, such as Confidential, Personal, etc.
- Excessive Postage
- Hand Written or Poorly Typed Addresses
- Incorrect Titles
- Title but No Names
- Misspellings of Common Words
- Oily Stains or Discoloration
- No Return Address
- Excessive Weight
- Rigid Envelope
- Lopsided or Uneven Envelope
- Protruding Wires or Tinfoil
- Excessive Securing Material such as Masking Tape, String, etc.
- Visual Distractions

Boarding Tickets

- The latest trend: print your boarding pass from the airline's web site
  - Security on Frankfurt/Main airport (FRA) relies on all boarding tickets (Internet or not) to be barcoded
  - The security checkpoint is central, therefore, it is not airline specific
- This implies that:

1. The security checkpoint may not know all checked in passengers, since it would have to have a backend connections to all airlines represented in FRA.
2. Therefore, the validity must be in the barcode


Bitte auf kurzfristigen Wechsel des Ausgangs achten
Please observe gate changes at short notice
etix etkt etix etkt
ELECTRONIC TICKET 220 1796364677
LUFTHANSA
LINDNER/FELIX MR
FRA LH 194 G 12DEC
TXL
ECONOMY 091
Bordkarte/Boarding Pass
Name of passenger
LINDNER/FELIX MR
ETKT 220 1796364677
FRA
TXL
LUFTHANSA M/M
Lufthansa
There's no better way to fly.
Bitte auf kurzfristigen Wechsel des Ausgangs achten
Please observe gate changes at short notice
etix etkt etix etkt
ELECTRONIC TICKET 220 1796364602
LUFTHANSA
LINDNER/FMR
FRA LH 190 C 26OCT
TXL
1D
BUSINESS 273
Bordkarte/Boarding Pass
Name of passenger
LINDNER/FMR
ETKT 220 1796364602
FRA
TXL
LUFTHANSA
Carrier Flight No./Class Date
LH 190 C 26OCT
Bitte auf kurzfristigen Wechsel des Ausgangs achten
Please observe gate changes at short notice
etix etkt etix etkt
ELECTRONIC TICKET 220 1796364671
LUFTHANSA
LINDNER/FELIX MR
TXL LH 270 G 30NOV
CGN
16C
ECONOMY 036
Bordkarte/Boarding Pass
Name of passenger
LINDNER/FELIX MR
ETKT 220 1796364671
TXL
CGN
LUFTHANSA M/M
Carrier Flight No./Class Date
LH 270 G 30NOV
Bitte auf kurzfristigen Wechsel des Ausgangs achten
Please observe gate changes at short notice
etix etkt etix etkt
ELECTRONIC TICKET 220 1796364602
LUFTHANSA
LINDNER/FELIX MR
TXL LH 195 C 23OCT
FRA
4G
LH 195 /154
BUSINESS 154
Bordkarte/Boarding Pass
Name of passenger
LINDNER/FELIX MR
ETKT 220 1796364602
TXL
FRA
LUFTHANSA M/M
Carrier Flight No./Class Date
LH 195 C 23OCT
Gate
Boarding
Seat

Boarding Tickets

Original

Bitte halten Sie diese Einsteigekarte und ein gültiges Personaldokument beim Einsteigen bereit.
Please be prepared to present your boarding pass and a personal document at the gate.

Air Berlin Einsteigekarte | Boarding Pass

Airline	Name of passenger		FQTV No.	Ticket No.
Air Berlin	censored			7451796364626

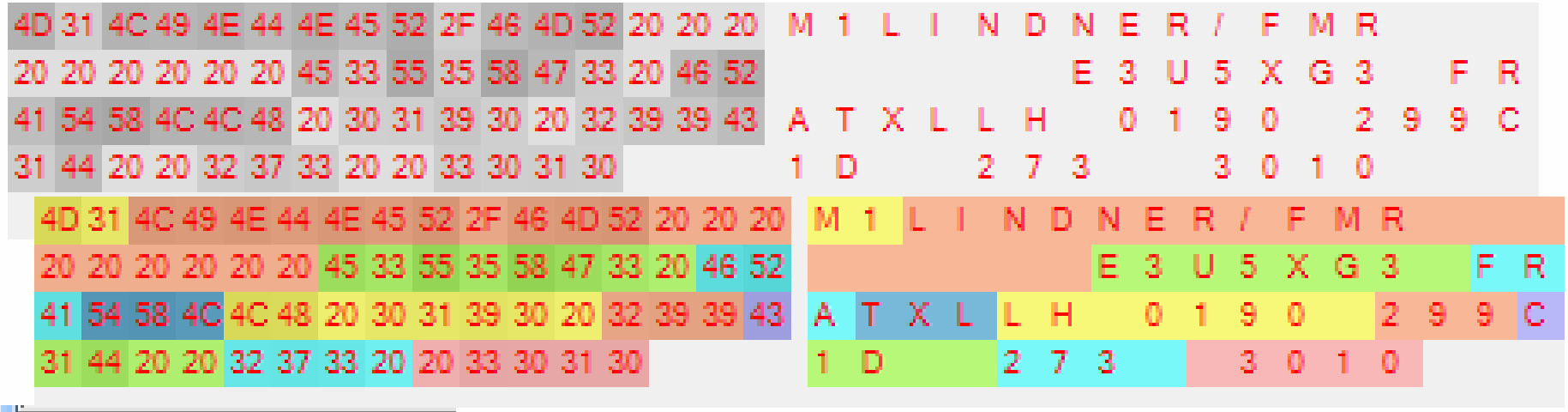
From	To	Flight no.	Date	Departure time
Berlin (Tegel)	Münster-Osnabrück	AB6464	29Oct2007	08:05

Gate	Boarding time	Seat	Class / Security number
C50	07:35	02A	003

Check your final gate information.
Bitte achten Sie auf kurzfristigen Wechsel der Flugsteige.

Boarding pass produced: 28.10.2007 19:29 CET

Boarding Tickets



Boarding Tickets

- Everything in the ticket barcode can be either predicted or ignored.
- We can make arbitrary boarding tickets now. Oops.

```
M1YYYYYYYY YYYYYYY              TXLFRAAB 6563 264 06C 041   00
M1LINDNER/FELIXMR      E77      MUCTXLLH 0232 271M021D0077 300
M1XXXXXXXXX XXXXXXXX            TXLFMOAB 6464 302 02A 003   00
M1LINDNER/FMR          E3U5XG3  FRATXLLH 0190 299C1D  273  3010
M1LINDNER/FELIX MR     EY2KI8G  TXLCGNLH 0270 334M16C 036  3010
M1LINDNER/FELIX MR     EYMZSB3  TXLFRALH 0195 296C4G  154  3010
M1LINDNER/FELIX MR     E3HUYFI  FRATXLLH 0194 346M32C 091  3010
```

Baggage Tracking

- Works by logically attaching a 1D barcode to your boarding pass
  - Baggage is routed in the airport delivery systems depending on the barcode on it
- With online boarding, you connect an piece of baggage to your boarding pass by dropping it off at the counter
  - Assumed it was your boarding pass to begin with

Wheelie of Fortune

Copy Pass

Ernst Agent

Abdul bin Scheusal

Boarding Pass

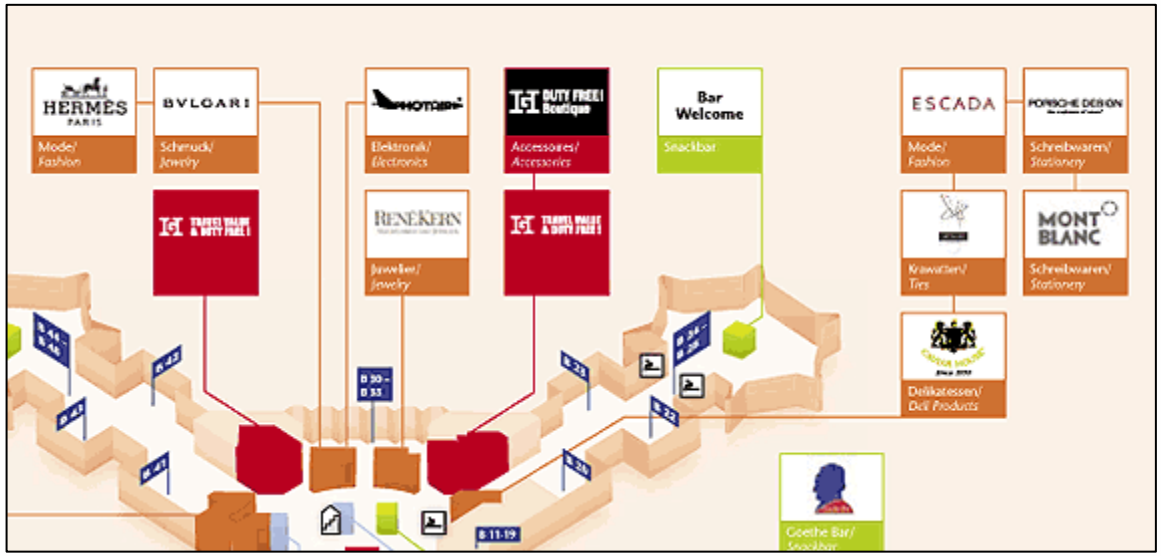
X-Ray

Brain- and Fearless security (BaFe)

TERRORIST!!1!

Baggage Tracking: Fix Recommendation

- Evil water bottles are already illegal
  - Not if you buy them for € 3,50 after security
- Simply make Luggage illegal!
  - The infrastructure for the traveler is already there!



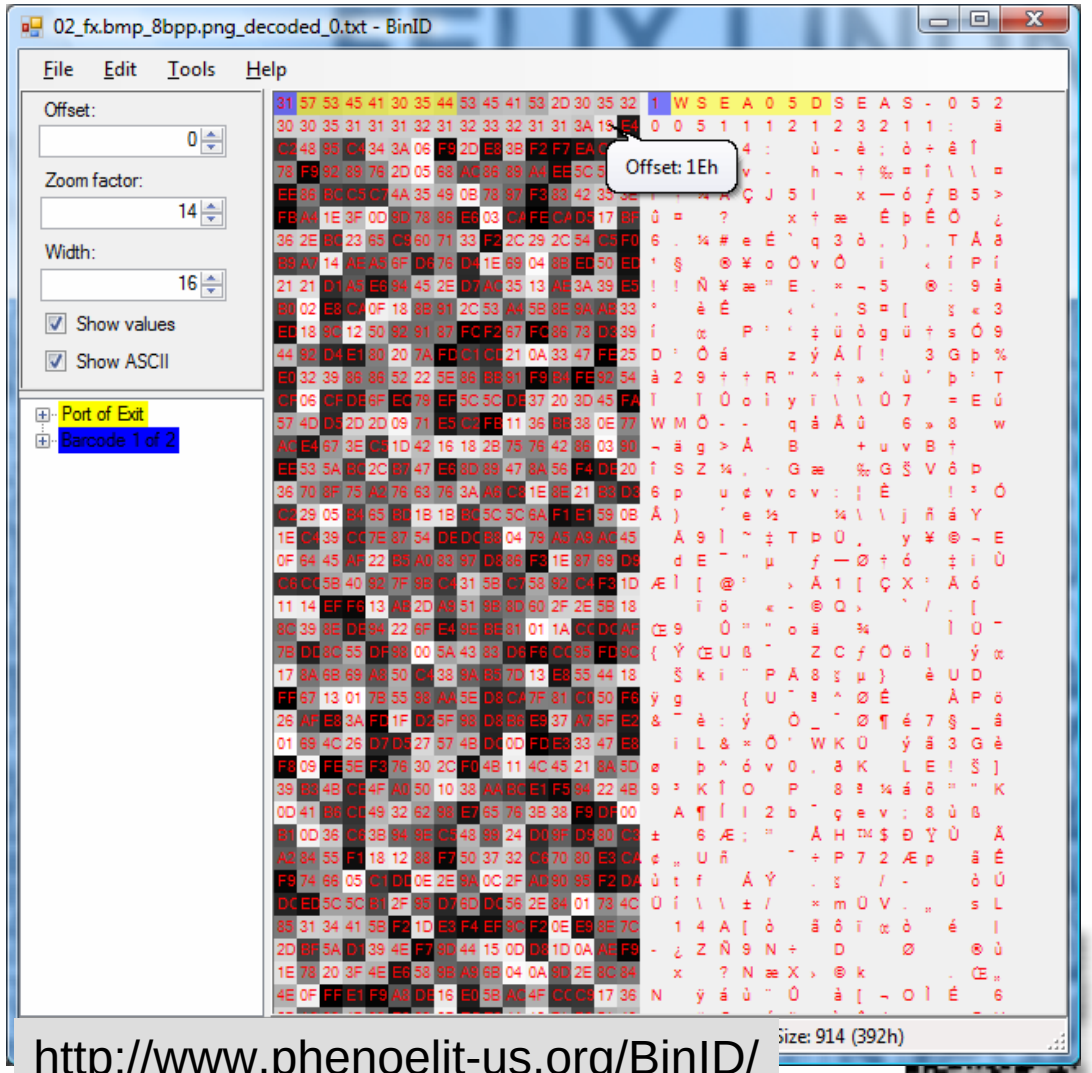
Frankfurt Airport Shopping

Unsolved Cases

- Deutsche Post
- Deutsche Bahn
- US Immigration

An Invitation

- BinID will be released to those interested
  - Please provide feedback
- I will decode any barcode our commercial software can handle and send you the result
  - If we get swapped, we will automate it



http://www.phenoelit-us.org/BinID/

Principles of secure barcode applications

- Consider the barcode like a browser cookie
  - It may be intercepted, copied, modified, lost, etc.
- If you can only use 1D, make sure it represents an unpredictable internal ID and nothing else.
- If you can use 2D, use real crypto.
  - It doesn’t cost you more.
  - It may provide non-repudiation in both ways.
- Make sure your process works
  - If your process trusts the barcode, you are toast
  - Make sure the connection between the tag and the item works. There is no browser to cooperate with.
  - Never trust the printed number!

Thank you, as always!

FX of Phenoelit
fx@phenoelit.de

Shouts: Phenoelit, Fixer, Halvar & Zynamics, Frank Boldewin, David, Manu & Geraffel, twist4, Scusi, CCCB, NoLogin and many many others