TROOPERS

MAKE THE WORLD A SAFER PLACE

TROOPERS 2013

QR-CODE SECURITY

PETER KIESEBERG
SBA RESEARCH GGMBH

Agenda

- Introduction to QR-Codes
- Phishing using malicious codes
- Manipulation of existing codes
- Countermeasures
- Field Study
- Steganography

- Discussion

Motivation

- Somewhat forced on us … see them everywhere
- Not human readable …
- … but seen them getting scanned
- Talk on barcode-abuse by FX/Phenoelit (DefCon 16)
- Samsung USSD-debacle

Planned …

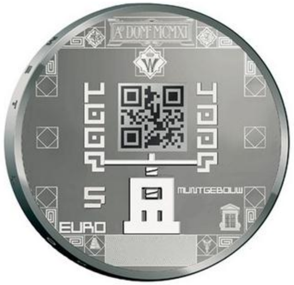
DENSO WAVE (Japan)
1994

Logistics for components
at Toyota

Today …

Bag with QR-Code[1]

Advertisement[3]



Netherlands: 5 € Coin[2]

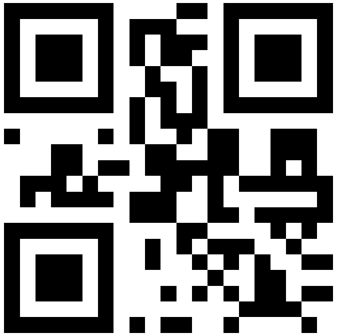
[1] http://www.printshop.at

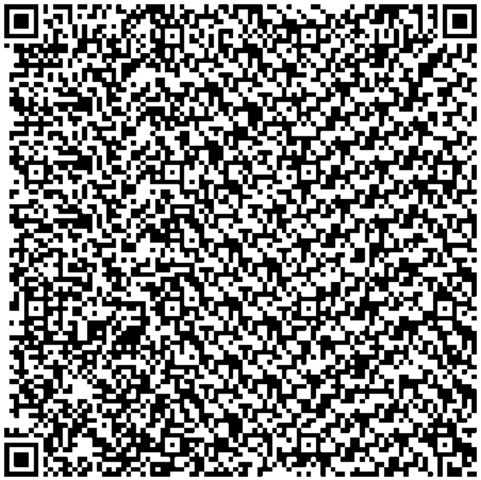
[2] http://2d-code.co.uk/

[3] http://www.onetoone.de

QR-Code Characteristics

- Different sizes: Type 1 to 40 (21 – 177 modules width)





- Different source encodings:
  - Numbers, alpha-numeric, 8-bit, Kanji, ECI-encodings
  - mixing modes / own modes are possible

QR-Code Characteristics

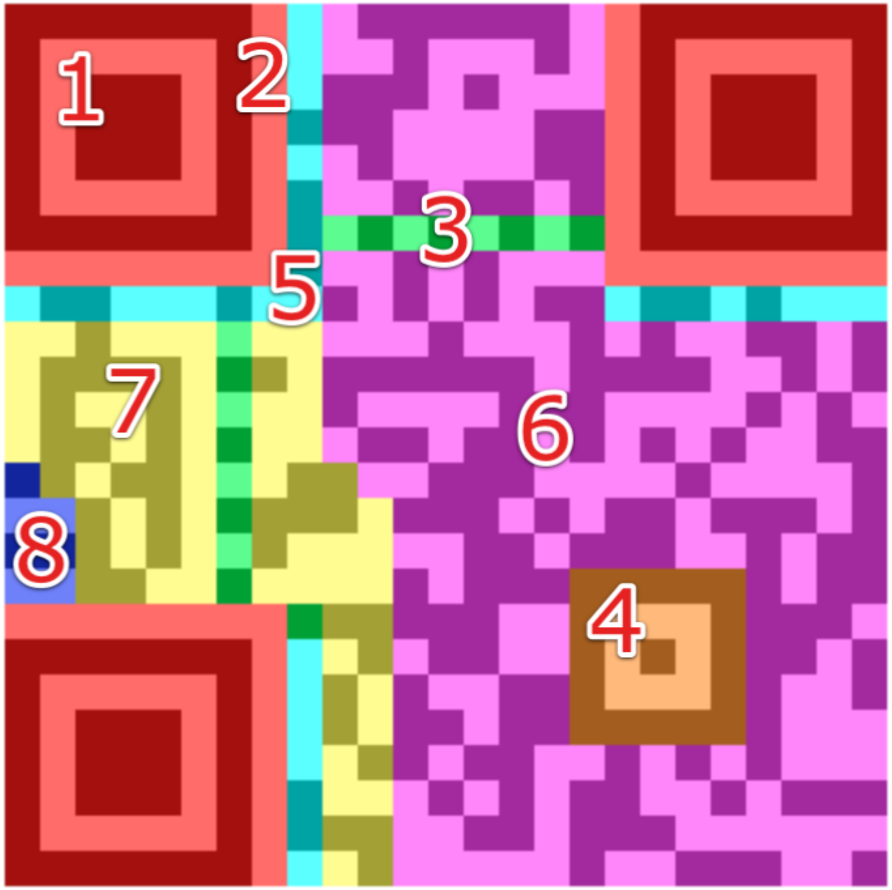
- Immune to rotation
- Can cope with a fair bit of distortion

- Provides error correction

→7%, 15%, 25%, 30% - levels (avg.), often higher

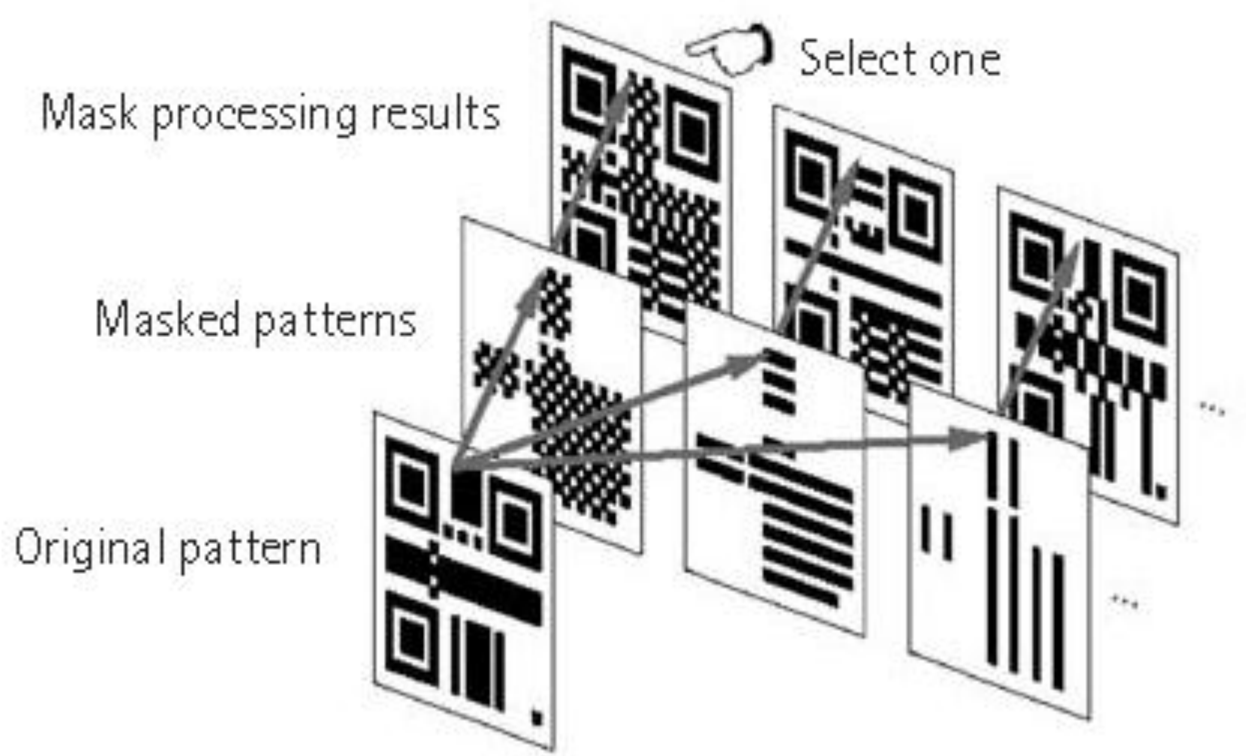
- Free standard
- Fair amount of decoders available.

QR-Code Structure



1. Finder Pattern
2. Separators
3. Timing Pattern
4. Alignment Patterns
5. Format Information
6. Data
7. Error Correction
8. Remainder Bits

Masking



Source: Tan Jin Soon, Synthesis Journal 2008

Malicious USSD-Codes

- Unstructured Supplementary Service Data
- GSM
- Communication between cell phone and provider
- Phone configuration, mobile-money services, location-based content services, …
- Real-time connection
- Example: *#06# (show IMEI)

- Talk by Ravishankar Borgaonkor on TelcoSec-Day

Possible threats

- Actual codes often depending on phone vendor
- Android: USSD like Number in dialer
- Website with iframe containing „tel:<USSD>“

- Samsung: Kill-Codes for cell-phones
  - Silent PUK-changes – 10x wrong → SIM-card destroyed
  - Silent factory reset

- For more information: Ravi.

USSDs via QR-Codes

- You need:
- The suitable USSD-Code
- A QR-Code-generator
- Android-User with App that executes QR-Codes automatically and a dialer that dials automatically

- Have fun: „tel:<USSD>“

- QR Droid: Detects USSDs

Phishing with QR-Codes

- Background: Marketing campaigns
- User scans the QR-Code on the street and logs on the page using his/her account information
- But: Is the QR-Code legit?

www.yah00.de

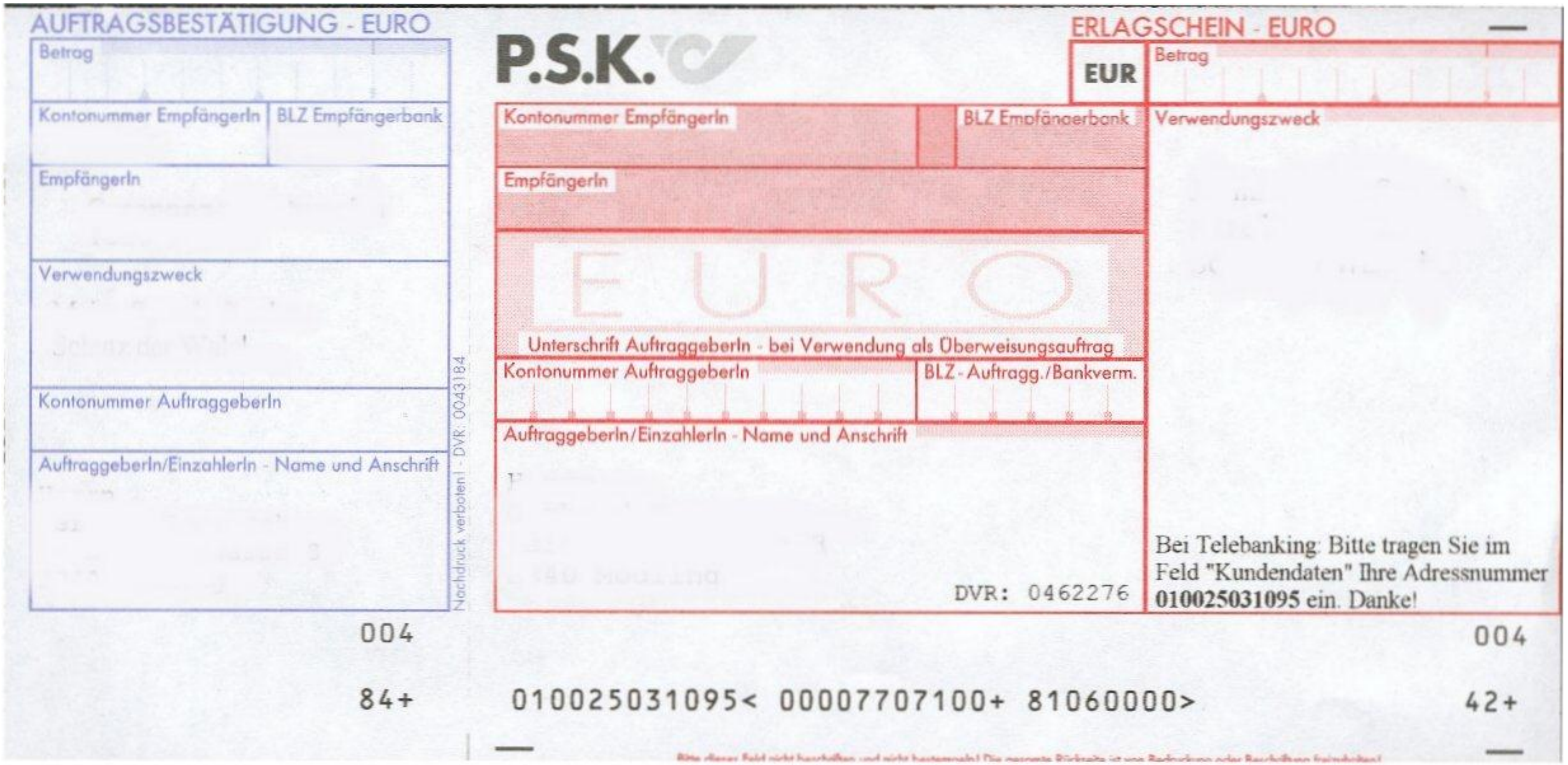
Maybe shoud have chosen the other pill...

BCD
001
1
SCT
RLNWATWW
Wrong pill society
AT611904300234573201
EUR10

Donate - A kitten for Neo

8189-2914-2104-8081-8825

A more interesting example …



AUFTRAGSBESTÄTIGUNG - EURO

Betrag

Kontonummer EmpfängerIn | BLZ Empfängerbank

EmpfängerIn

Verwendungszweck

Kontonummer AuftraggeberIn

AuftraggeberIn/EinzahlerIn - Name und Anschrift

Nachdruck verboten! - DVR: 0043184

004

84+

P.S.K.

ERLAGSCHEIN - EURO

EUR | Betrag

Kontonummer EmpfängerIn | BLZ Empfängerbank

EmpfängerIn

EURO

Unterschrift AuftraggeberIn - bei Verwendung als Überweisungsauftrag

Kontonummer AuftraggeberIn | BLZ - Auftragg./Bankverm.

AuftraggeberIn/EinzahlerIn - Name und Anschrift

DVR: 0462276

Verwendungszweck

Bei Telebanking: Bitte tragen Sie im Feld "Kundendaten" Ihre Adressnummer **010025031095** ein. Danke!

004

010025031095< 00007707100+ 81060000>

42+

Bitte dieses Feld nicht beschriften und nicht bestempeln! Die gesamte Rückseite ist von Bedruckung oder Beschriftung freizuhalten!

The Stuzza-Standard - Payment orders via QR-Codes

Data field	Content	Mandatory
Service ID	„BCD“	Yes
Version	„001“	Yes
Encoding	UTF-/ISO-Encoding of Data	Yes
Function	„SCT“	Yes
BIC	BIC	Yes
Recipient	Recipient Account Holder	Yes
IBAN	IBAN	Yes
Currency + Amount	999.999.999,00€ max.	No
Purpose	Reference or Text	No
Reference/Text	35 Bytes/140 letters	No
Displayed Message	70 letters	No

Payment orders via QR-Codes

- Stuzza – Association for Cooperation in Payment Transfers, goal: Development of payment transfers

- First version of a standard for payment orders via QR-Code: January 2012, current: 1.11
- Provided to the European Payment Council for standardization

- Standard and BCD-Checker available on homepage www.stuzza.at

Maybe shoud have chosen the other pill...

BCD
001
1
SCT
OPSKATWW
Peter Kieseberg
AT226000000136439140
EUR10.00

Donate - A kitten for Neo

8189-2914-2104-8081-8825

CAT

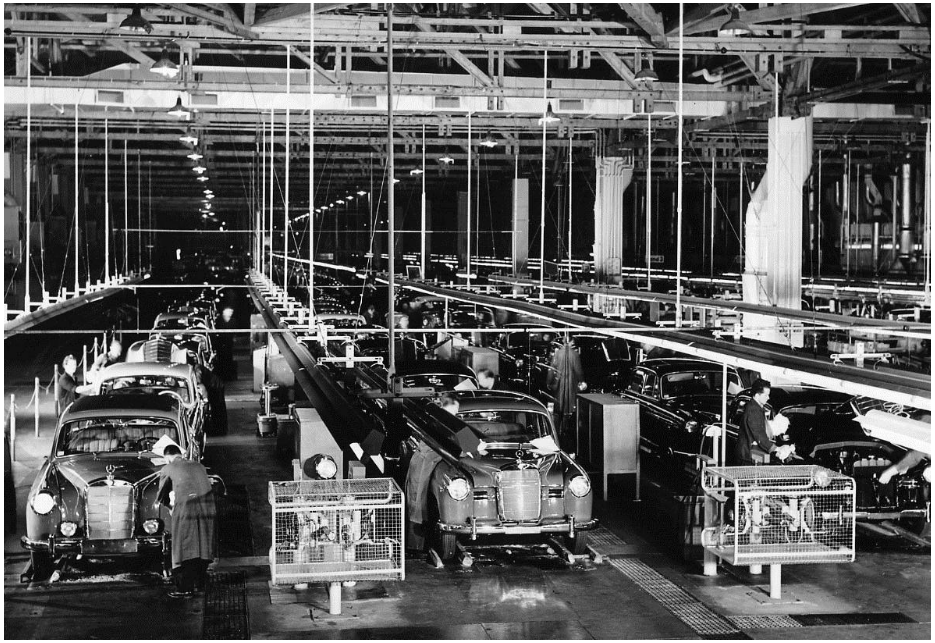
- City-Airport-Train
- Rather expensive
- Check in: train-station

- Online-Tickets contain QR-Code
- Additionally: Name and Number

- Pattern in the number (direction, day)

What about production lines?

- Inducing Code?
- Proprietary Systems



- Try to get our hands on one soon – test system only

Phishing with a pencil …

- Overwriting deployed codes
- Only one color (e.g. black marker)
- Search for useful parts in QR-Codes

Targets for Manipulation – the mask?

- The Masks
  - Stored in the Format Information (5)
  - Eight different masks
  - Used to generate a 50:50-distribution of black and white modules
  - Changing the mask changes the whole data and error correction part
  - Encoded separately using a very strong BCH-Code
  - Maybe useful as a basis for further attacks.

Encodings and count indicators

- The character encoding
  - Defined at the beginning of the data part
  - Complete change of data block, maybe interesting for code-injections
  - Especially interesting when using mixed modes

- The character count indicator
  - Defined at the beginning of each data block
  - Defines length of the block
  - Interesting for overflow/underflow-attacks

The largest parts

- Data part and error correction (6, 7, (8))
  - Make up the largest part of the code
  - Data is encoded using a Reed-Solomon-Code

- Reed-Solomon-Codes
  - Subfamily of BCH-Codes
  - Designed to detect and correct random symbol errors
  - Optimal and systematic Code
  - Different levels of error correction (L, M, Q, H) → (7, 15, 25, 30) %

BCH-Codes

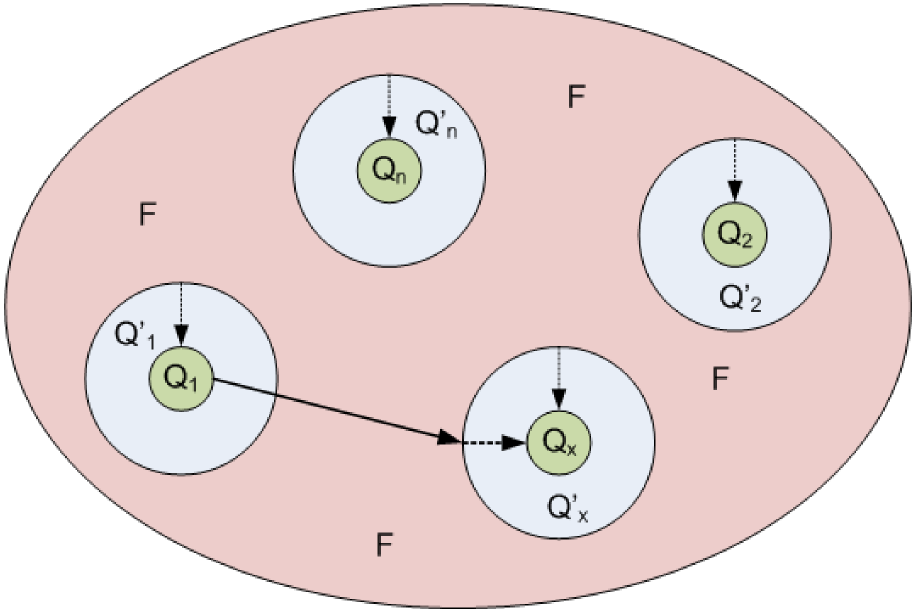
- Bose-Chaudhuri-Hocquenghem-Codes
- Works with polynomial multiplication or division → efficient over fields with characteristic of 2

- g(x) … generator polynomial
- a(x) … source encoded data
- c(x) … channel encoded data

- c(x)=a(x)*g(x)

With a little help from the error correction

A little difficulty: One color only.



→ Don‘t need a direct hit.

Attack outline

1. Attacker scans code $D_o$and retrieves message M_0
2. Generate i messages M_i with phishing URLs with Q_i(same version and mask)
3. Construct the change matrix

$$C_i = (c_{i,j}) = \begin{cases} c_{i,j} \coloneqq 1, white \ \rightarrow black \\ c_{i,j} \coloneqq -1, black \ \rightarrow white \\ c_{i,j} \coloneqq 0, no\ change \end{cases}$$

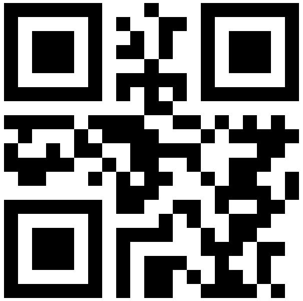
Attack outline

4. Remove impossible solutions, i.e. where $|black \rightarrow white| > e$, with e … error correction capacity.
5. Sort remaining solutions by least effort for the coloring, i.e. by $|white \rightarrow black|$ in ascending order.
6. Recolor the original QR-Code

http://yghqo.at

Choosing random modules

1. The attacker scans the QR-Code $Q_0$and retrieves M_0
2. r white modules are chosen randomly and set to black, $r > e$, resulting in QR-Codes Q_i containing random messages M_i
3. Step two is repeated several times (e.g. 100)
4. Attacker chooses M_i and colors Q_0 to resemble Q_i



http://yihoo.com (5)

http://yahgo.com (5)

http://yahno.com (6)

...

http://yahmg.kom

http://?phoo.co}

http://yahok.com

http://yahoo?agm

http://xexn/.com

http://yehom.com

http://yahgo.com

http://yAhoo.agm

http://Yahoo.com

http://yah/o.com

http://yahoo.?mm

http://yaxoo,coM

http://yihoo.com

http://y!hoo.c□?

http://y?h/o.kmi

http://yaioo/Gom

...

Your own personal everything.
Make Yahoo! your home.
Y!

Another approach … outline

- Remember Stuzza
- Some parts are free, some fixed (line breaks, BIC, IBAN)
- m_1, m_2, $b(m_1)$, $b(m_2)$

  → $b(m_1 \oplus m_2) = b(m_1) \oplus b(m_2)$
- Use Gauss-Jordan elimination for targeted changes

  → Try to change some of the desired modules directly

- See QArt-Codes: http://research.swtch.com/qart

Another approach … downside

- Not able to change single modules
- Not able to change all modules – control-modules contain the data we need for the payment
- Additional: Masking

- Comes down to brute-forcing …

→ Choose older approaches without changing sensitive fields.

The central question …

The question is …

… who cares?

Field Study

- Field Study on acceptance of QR-Code and user awareness concerning security
- Publishing QR-Codes with link to a study on public places
- Five Cities
  - Athens (already deployed)
  - Helsinki (already deployed)
  - Paris (already deployed)
  - Tokyo (still ethical discussions)
  - Vienna (currently deployed)

Field Study

- Plain Stickers

- QR-Code with short description

Participate

in our security awareness survey 🧁

- QR-Codes with nice pics

Field Study

- Every QR-Code is unique
- Contains:
  - Unique ID
  - City
  - Deployment type
  - Link to the survey
- Deployment
  - Bus stops
  - Toilets
  - Campus
  - Random places (ATMs, vending machined, parking machines)

Field Study

- Automatically logging scan
  - Logging QR-Code and scan-time
  - Retrieve information using Google Analytics
  - Country, City, Browser, OS, Service Provider, New Visitor
  - All personal data is removed

- Redirecting User to Survey
  - Show disclaimer with explaination (Who, What, Anonymity)
  - Show Survey (7 questions, multiple choice)
  - Measure time to complete survey (curr. ~ 3-4 min.)

Survey questions

- Why did you scan this QR-Code?
- Did you have any doubts or malicious expectations before scanning this QR-Code?
- When scanning a code, do you check the web address before visiting the link?
- Have you ever been a victim of a phishing attack?
- How often do you scan QR-Codes?

- Age/Gender

Results? No, but …

- Currently deployment phase …
- ~3-4 minutes/survey
- High acceptance of the survey
- … Kitty seems to be winning

Countermeasures

- Always show links
- Additional option: Blacklisting
- Look at the ad – detect tampering
- Number/Distribution of b/w-modules (Mask!)

- For USSDs: Shouldn‘t be treated like numbers
- For Samsung: Use additional dialer

- Payment orders: Additional verification procedure?

Conclusion

- Trivial attacks … but new vectors
- Link paper ads to the digital world
- Targeting unsuspecting users

- Delicate applications are fashioned (stuzza)

- QR-Codes can be used for many things

Future Work … if there is time

- Many things left in the spec
  - Special / User-defined encoding
  - Continuous QR-Codes
  - Buffer under/overflows
  - Working payment-apps

Thanks go to

- Colleagues
  - Sebastian Schrittwieser
  - Katharina Krombholz
  - Ioannis Kapsalis
- Friends
  - Athens, Helsinki, Paris, Tokyo, Vienna

Thank you!

Thank you

pkieseberg@sba-research.org
www.sba-research.org