QR-Inception: Barcode in Barcode Attacks

Adrian Dabrowski
adabrowski@sba-research.org
adrian.dabrowski@tuwien.ac.at

ACM CCS 2014 ; 2014-11-07

Polyglots

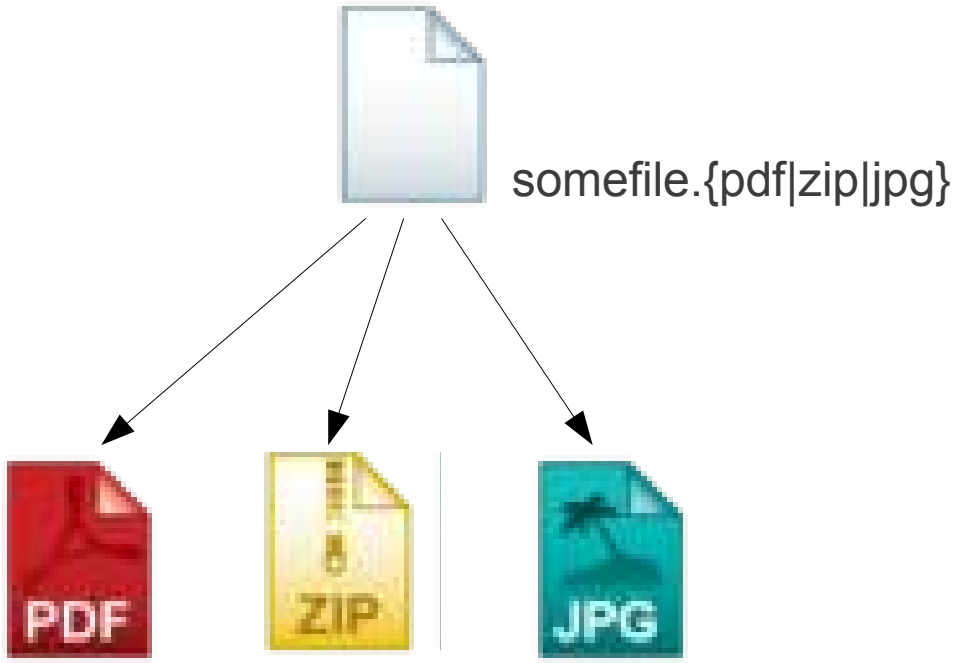
- Source code that is valid in multiple programming languages
- Simple one: (Perl+C)

```
#include <stdio.h>
#define do main()
do {
   printf("Hello World!\n");
}
```

- More: http://www.nyx.net/~gthompso/poly/polyglot.htm

Binary Polyglots

- One file



- Valid as **PDF** **ZIP** **JPEG** simultaneously
- e.g. new editions of POC||GTFO

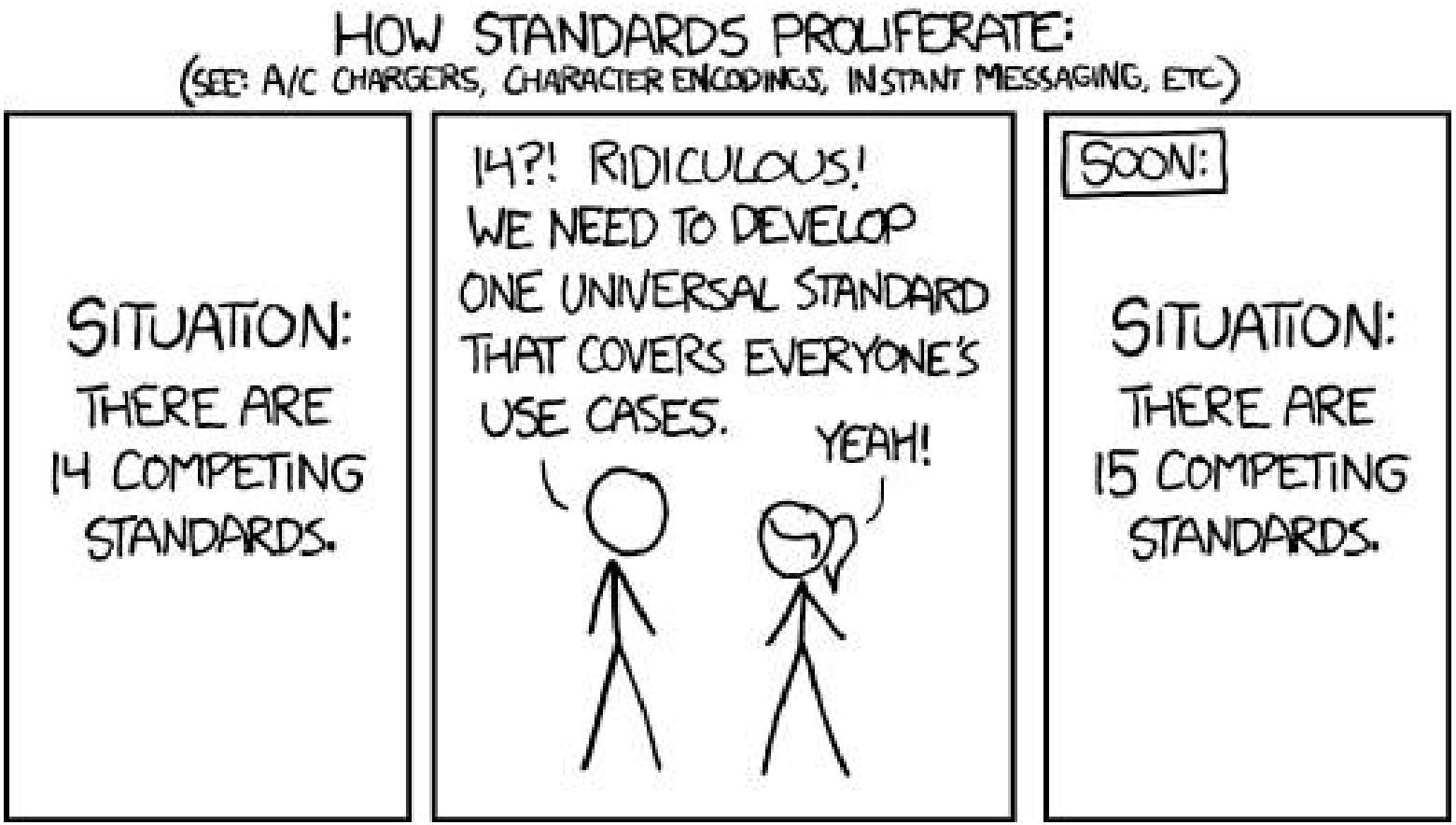
Ange Albertini, http://code.google.com/p/corkami/#Binary_files

“Ambiguity is Insecurity”

– L. Sassaman, M. L. Patterson

- File and network protocol parsing
  - AV scanner
  - Firewalls
  - Security Checks
  - …
- Does it work with Barcodes as well?

2D Barcodes ?

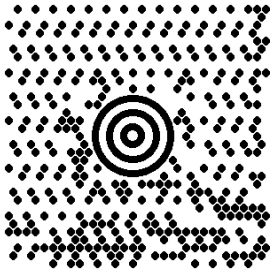


http://xkcd.com/927/

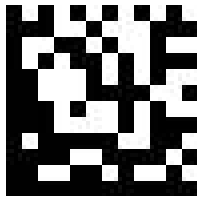
(some) 2D Barcodes

PDF417

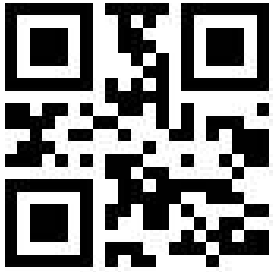
Aztech



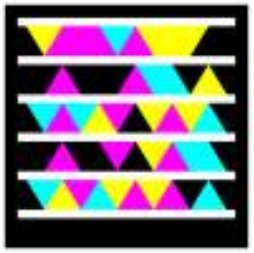
Maxicode



Data Matrix



Quick Response Code



Microsoft Tag
(High Capacity Color Barcode)

3-DI

Shotcode

Only harmless fun?

- 2012: USSD-Codes in Tel:-URLs encoded in Barcodes could wipe a phone.
- Generate Premium-Rate SMS
- URLs can trigger exploits in Web-Browser, Renderer, OS, code Injection, ...
- Used for financial transactions

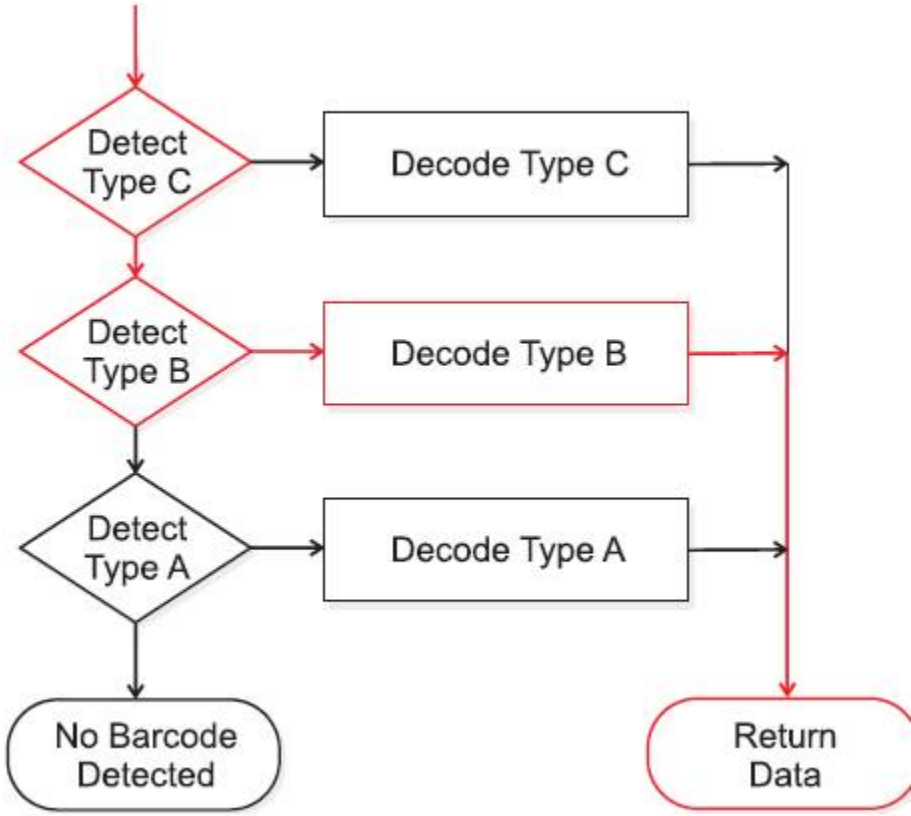
Some attack scenarios

What if we could construct a barcode that decodes to different values by different clients?

- Tailored exploits for certain plattforms/readers (e.g. only some phones get wiped)
- Donation-QR diverts small amount of users to different target account
- In logistics, package handlers read different destinations – creating e.g. loops or fee fraud.

QR Inception

- Can we construct a barcode that complies to multiple standards?
- What attacks are possible?
- Why does it work?

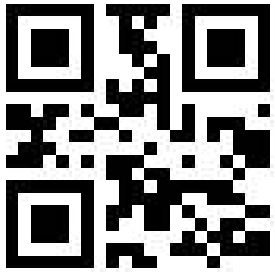


Building Multi-Standard Barcodes

- Limit to quadratic pixels

Aztech

Data Matrix

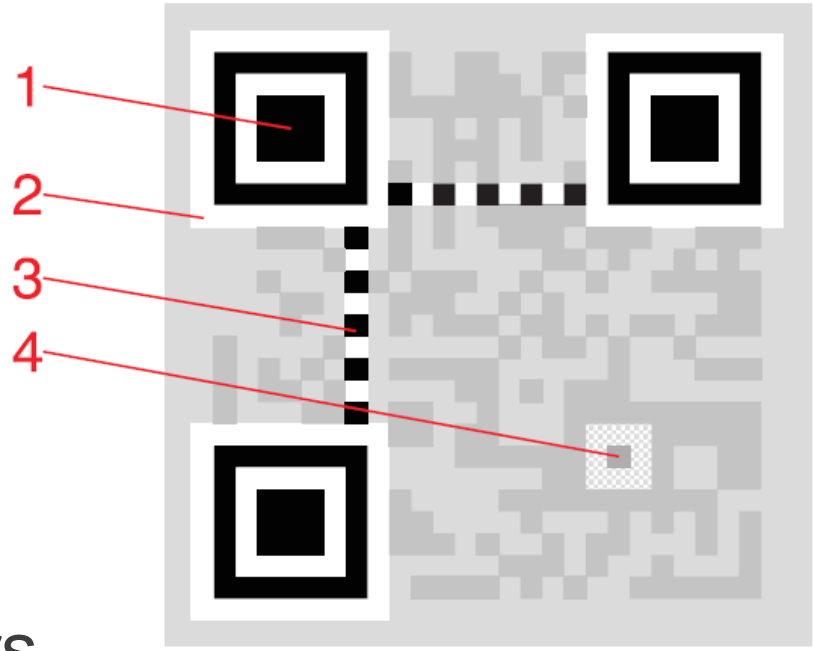


Quick Response Code

- Exploit error correction
  - QR has the most robust one
  - Include smaller code into a bigger one, let ECC handle the rest
- Mind the quiet zone

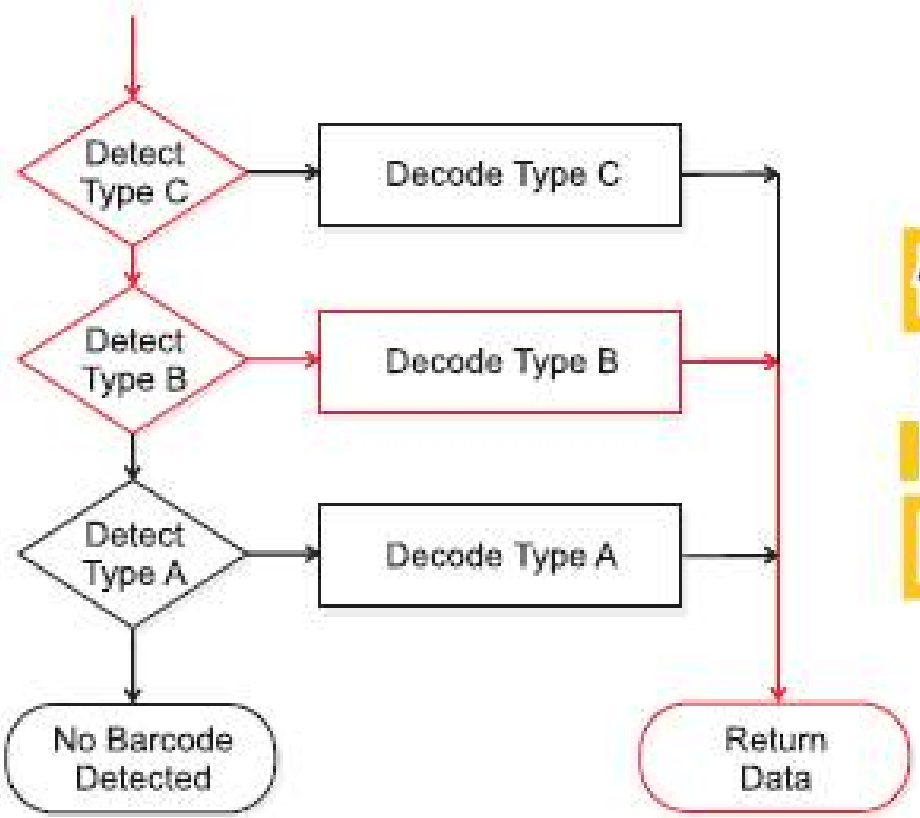
QR Code as host

- QR hast most robust ECC (of these 3 symbologies)



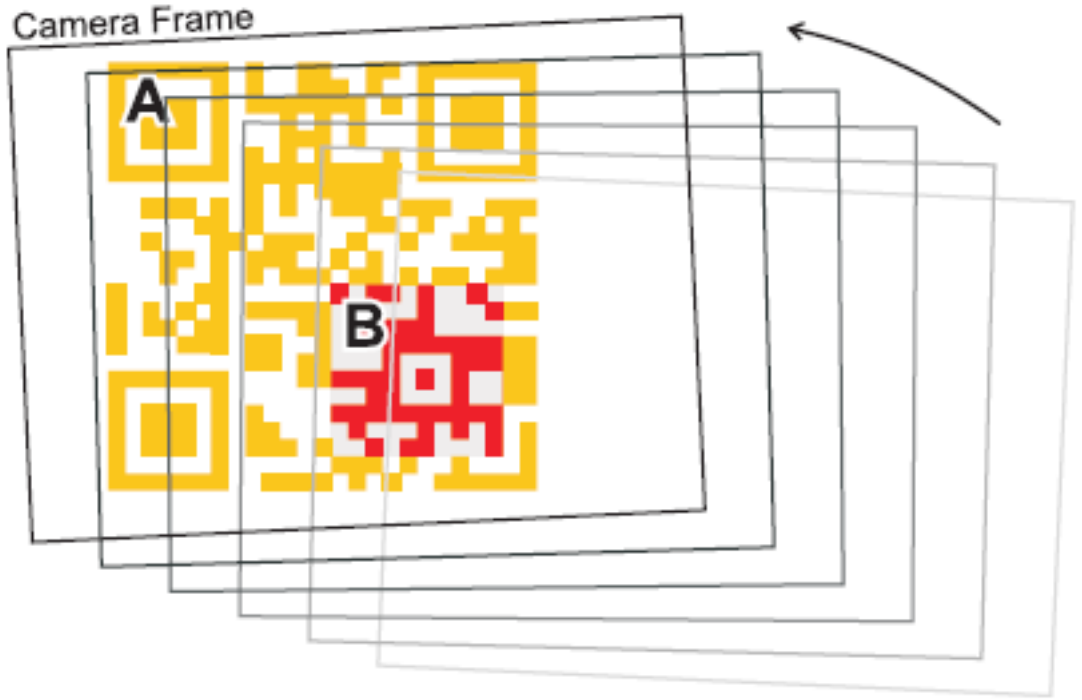
1) location markers
2) quiet zone
3) timing pattern
4) alignment markers

Type 1: Decoding sequence



Type 2: incomplete capture

- Sliding over the barcode will make the smaller inner barcode fully visible before the entire (outer) barcode



Testing

OS/Type	Name	QR	Data Matrix	Aztec	Auto-load URLs
iPhone	NeoReader [21]	✓	✓	✓	✓
	Qrafter [16]	✓	✓	✓	✗
	i-nigma [4]	✓	✓	✗	✗
	QR Code Reader and Scanner [27]	✓	✓	✓	✓
	ScanLife [25]	✓	✓	✗	✗
Android	ZXing Barcode Reader [31]	✓	✓	✗	(✗)[1]
	UberScanner [30]	✓	✓	✓	✗
	ScanLife [26]	✓	✓	✗	✓
	i-nigma [5]	✓	✓	✗	✗
	AT&T Code Scanner [9]	✓	✓	✗	✓
	NeoReader [22]	✓	✓	✓	✗
	ShopSavvy [28]	✓	✓	✗	✓
Handheld	Symbol DS6708 [13]	✓	✓	✓	–

Some examples: Aztec

App/Device	Outer	Inner
NeoReader	✓	✓pref.
Qrafter	✗	✗
i-nigma	✓	–
QR Code R.S.	✓	✗
ScanLife	✓	–
ZXing B.S.	✓	–
UberScanner	✓	✓
ScanLife	✓	–
i-nigma	✓	–
AT&T Code S.	✓	–
NeoReader	✓	✓
ShopSavvy	✓	–
DS6708	✓	✓

DM in QR

App/Device	Outer	Inner
NeoReader	✓	✓
Qrafter	✓	✗
i-nigma	✓	✗
QR Code R.S.	✓	✗
ScanLife	✓	✗
ZXing B.S.	✓	✗
UberScanner	✓	✗
ScanLife	✓	✗
i-nigma	(✓)	✗
AT&T Code S.	✓	✗
NeoReader	✓	✓
ShopSavvy	✓	✗
DS6708	✓	✗

App/Device	Outer	Inner
NeoReader	✗	✓
Qrafter	✓	✓
i-nigma	✓	✓
QR Code R.S.	✓	✗
ScanLife	✓pref.	✓
ZXing B.S.	✓	✓
UberScanner	✓	✓
ScanLife	✓	(✓swipe)
i-nigma	✓	✓
AT&T Code S.	✓	(✓swipe)
NeoReader	✓	✓
ShopSavvy	✓	✓
DS6708	✓	✓

QR in QR

App/Device	Outer	Inner
NeoReader	✓	✗
Qrafter	✗	✗
i-nigma	✓	✓
QR Code R.S.	✗	✗
ScanLife	(✓rot.)	✓
ZXing B.S.	✗	(✓swipe)
UberScanner	✗	(✓swipe)
ScanLife	✗	✗
i-nigma	✓	✗
AT&T Code S.	✗	✗
NeoReader	✓	✗
ShopSavvy	(✓)	✗
DS6708	✓	✓pref.

Many more examples in the paper.

Countermeasures

- Stringent decoding order
  - Root cause of decoding ambiguity
- Present user a visual excerpt
- Notification of all codes found
- Detect & display alien data in barcode
- Do not automatically retrieve & display target URL

QR-Inception: Barcode in Barcode Attacks

Adrian Dabrowski
adabrowski@sba-research.org
adrian.dabrowski@tuwien.ac.at

ACM CCS 2014 ; 2014-11-07