Practical exploitation of rounding vulnerabilities in internet banking applications

Adrian Furtunã, PhD, OSCP, CEH
adif2k8@gmail.com

Agenda

- Who am I
- Rounding vulnerabilities
- How to fix
- Exploitation techniques
- Digipass automation
- Demo

Who am I

- PhD in Information Security, OSCP, CEH
- Penetration tester at KPMG Romania
  - Web applications, internet banking
  - Network infrastructures
  - Mobile applications
  - Source code reviews
  - + some annoying stuff
- Teaching assistant at Information Security Master programs from Bucharest universities
  - Teaching penetration testing classes
  - Organizing Capture the Flag contests
- Always like to prove my point…

Rounding vulnerabilities

Real life example

- How much do you *really* pay?

Real life example

- How much do you *really* pay?
- What about:

  2.85e + 3.20e = 6.05e ?

Real life example

- How much do you *really* pay?
- What about:

  2.85e + 3.20e = 6.05e ?
- How much does the seller win from rounding?

Real life example

- How much do you *really* pay?
- What about:

  2.85e + 3.20e = 6.05e ?
- How much does the seller win from rounding?

- We are a bit vulnerable…

In Internet Banking apps

- Banks are vulnerable also

In Internet Banking apps

- Banks are vulnerable also
- Amounts are specified with two decimals:

	IBAN	Currency	Current Balance
Current Account	RO60[redacted]0210000001360445	EUR	0.67
Current Account	RO66[redacted]0210000001360434	RON	49.00

In Internet Banking apps

- Banks are vulnerable also
- Amounts are specified with two decimals:

	IBAN	Currency	Current Balance
Current Account	RO60[redacted]0210000001360445	EUR	0.67
Current Account	RO66[redacted]0210000001360434	RON	49.00

- What happens when you transfer 8.3436 EUR to your account?

  Amount += 8.34 EUR => Bank wins 0.0036 EUR

In Internet Banking apps

- Banks are vulnerable also
- Amounts are specified with two decimals:

	IBAN	Currency	Current Balance
Current Account	RO60[redacted]0210000001360445	EUR	0.67
Current Account	RO66[redacted]0210000001360434	RON	49.00

- What happens when you transfer 8.3436 EUR to your account?

  Amount += 8.34 EUR => Bank wins 0.0036 EUR

- What happens when you transfer 8.3478 EUR to your account?

  Amount += 8.35 EUR => Bank loses 0.0022 EUR

In Internet Banking apps

- Banks are vulnerable also
- Amounts are specified with two decimals:

	IBAN	Currency	Current Balance
Current Account	RO60[redacted]0210000001360445	EUR	0.67
Current Account	RO66[redacted]0210000001360434	RON	49.00

- What happens when you transfer 8.3436 EUR to your account?

  Amount += 8.34 EUR => Bank wins 0.0036 EUR

- What happens when you transfer 8.3478 EUR to your account?

  Amount += 8.35 EUR => Bank loses 0.0022 EUR

- Max to win/lose: 0.005 EUR / transaction

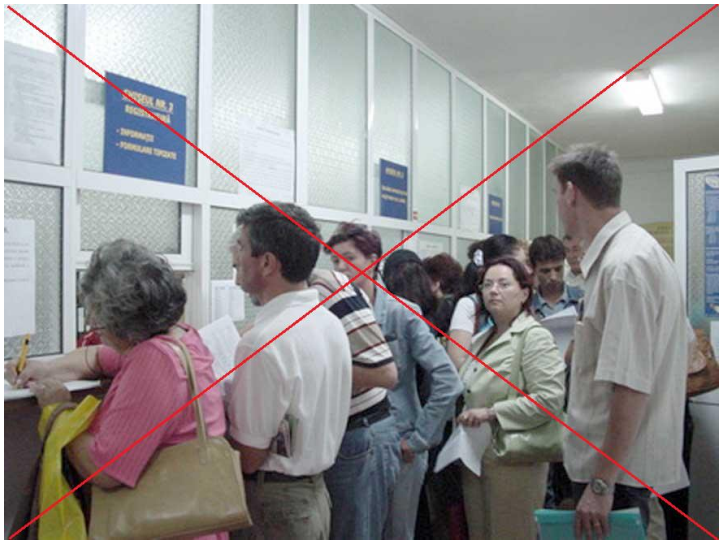
  Rounding is done to the closest value (two decimals)

How to always win?

- Let’s make transactions that will be always rounded in our favor

How to always win?

- Let's make transactions that will be always rounded in our favor
- How?
  - Foreign exchange transactions
  - Transfer between your own accounts having different currencies



Obtain a better exchange rate

- Transfer money between your own accounts (e.g. RON -> EUR)
- Specify how much RON you want to sell

RON	EUR	EUR (rounded)	Actual exchange rate (RON / EUR rounded)
4.40	1	1.00	4.40 **Official**
2	0.4545	0.45	4.44
1	0.2272	0.23	4.34
0.5	0.1136	0.11	4.54
0.05	0.0113	0.01	5
0.03	0.0068	0.01	3
0.023	0.0052	0.01	2.3 **The best**
0.02	0.0045	0.00	not good

100 * (0.023 RON -> 0.01 EUR) => 2.3 RON = 1 EUR

Example (1)

Generează raport | Filtrare/Căutare | Descarcă raportul

Contul * RO54[redacted]0000999902861827 [EUR]

Perioada * Alt interval — Trimite

13/02/2012 – 13/02/2012

Data	Detalii tranzacţie	Debit/Credit	Balanţă intermediară
[-] Toate tranzacţiile (Operatiuni:3)			
13/02/2012	Schimb valutar [redacted] Referinta: 7 Din contul: RO19[redacted]0000999902846549 Suma: 0,03 RON Rata: 4,40580	+ 0.01	0.03
13/02/2012	Schimb valutar [redacted] Referinta: 8 Din contul: RO11[redacted]0000999902861340 Suma: 0,03 RON Rata: 4,40580	+ 0.01	0.04
13/02/2012	Schimb valutar [redacted] Referinta: 9 Din contul: RO11[redacted]0000999902861340 Suma: 0,02 RON Rata: 4,40580	+ 0.01 EUR	0.05

Example (2)

ÉCHANGES VALUTAIRES

Client	**FURTUNA CONSTANTIN-ADRIAN**
CUI / CNP	
Compte vente:	RO78[redacted]0210000001360412 (RON)
Montant vendu:	0.025 RON
Compte achat:	RO72[redacted].0210000001360423 (EUR)
Montant acheté:	0.01 EUR
Rata de schimb	4.4614
Date d'ordre:	05/06/2013

La transaction a été introduite le 05/06/2013 à 13:10:44 heure par CONSTANTIN-ADRIAN FURTUNA
La transaction a été signée le 05/06/2013 à 13:10:59 heure par CONSTANTIN-ADRIAN FURTUNA (E)

autorisé. Referinta bancii: 021FT24131560016

Traité avec succès!

6/15/2013 6:15:33 PM

When is the best deal

- Foreign exchange transactions:
  - Specify how much you want to sell => destination will be rounded
  - Specify how much you want to buy => source will be rounded
- Best deal is when you can specify how much of the weaker currency you want to sell/buy because the stronger currency will be rounded

How much can I gain?

C1 = minimum amount of currency 1 that can be exchanged (e.g. 0.023 RON)
C2 = minimum amount of currency 2 that can be exchanged (e.g. 0.01 EUR)
Ex_b = exchange rate for buying C2 with microtransactions (e.g. 2.3)

Ex_b = C1 / C2

Ex_s = exchange rate for selling C2 (e.g. 4.4) – real exchange rate – fixed by the Bank

- z = y * Ex_s = (x / Ex_b) * Ex_s = x * **(Ex_s / Ex_b)**
- multiplication rate = Ex_s / Ex_b
- transactions required = x / C1

Currency	Multiplication rate	Initial amount (x)	Final amount (y)	Gain	Transactions required
RON	4.4 / 2.3 = 1.9	100 RON	190 RON	90 RON **~ 20 EUR**	100 / 0.023 = **4347**

Different exchange rates (buy / sell)

- Banks have different exchange rates for buying and for selling so they can always win
- Let's say…
  - Official exchange rate: 4.45
  - You buy from the Bank: 4.50
  - You sell to the Bank: 4.40
- But for small amounts it is not true!
  - I buy from the Bank (RON → EUR)
    - 0.45 RON / **4.40** = 0.102 EUR → 0.1 EUR
    - 0.45 RON / **4.50** = 0.100 EUR → 0.1 EUR
    - 0.45 RON / **4.60** = 0.097 EUR → 0.1 EUR
    - 0.45 RON / **4.70** = 0.095 EUR → 0.1 EUR

How to fix

How the Banks should protect themselves

- Limit the number of transactions that can be performed in a given time by a regular person
- Introduce a small fee for currency exchange operations (e.g. 0.01 EUR)
- Limit the minimum amount that can be transferred in a foreign exchange operation
- Monitor for suspicious transactions (numerous transactions, very small amounts)
- State in the contract that such transactions are illegal

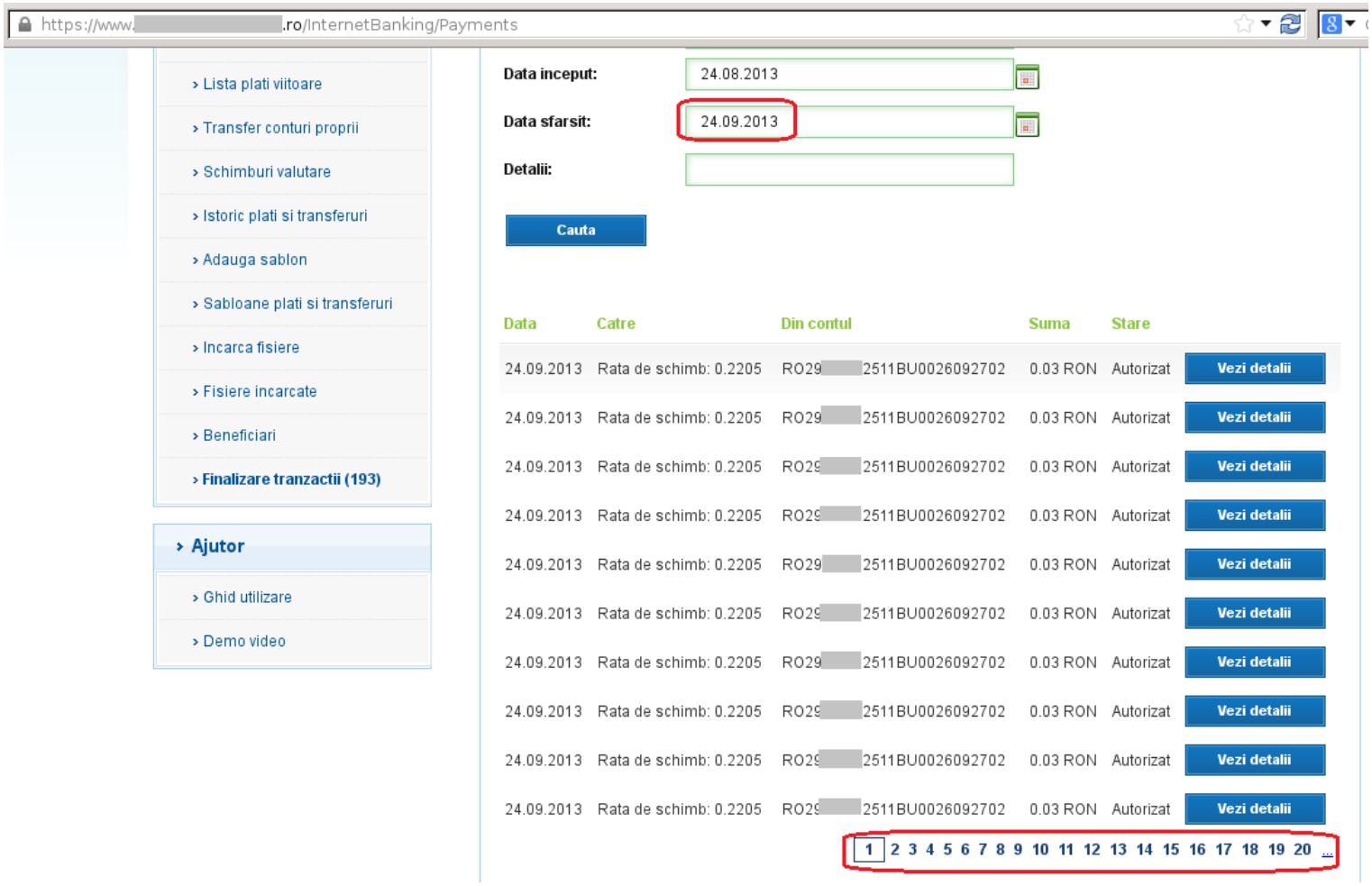
Exploitation techniques

General ideas

- Find a way to do lots of transactions in a relatively short time
- Transactions are made in two steps:
  - Initialization (can be automated)
  - Authorizing / Signing (requires human interaction)
- Automate / bypass transaction signing mechanism (digipass, SMS, token, etc)

Technique 0: No signing required ☺

- 3000 transactions, 90 minutes, 30 RON → 73 RON, gain ~10 EUR



Technique 1: Init lots and sign once

- Initiate lots of transactions automatically and sign once

Technique 1: Init lots and sign once

- Initiate lots of transactions automatically and sign once
  - Use Burp Suite to initiate transactions

Intruder attack 1

Attack Save Columns

Results | Target | Positions | Payloads | Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

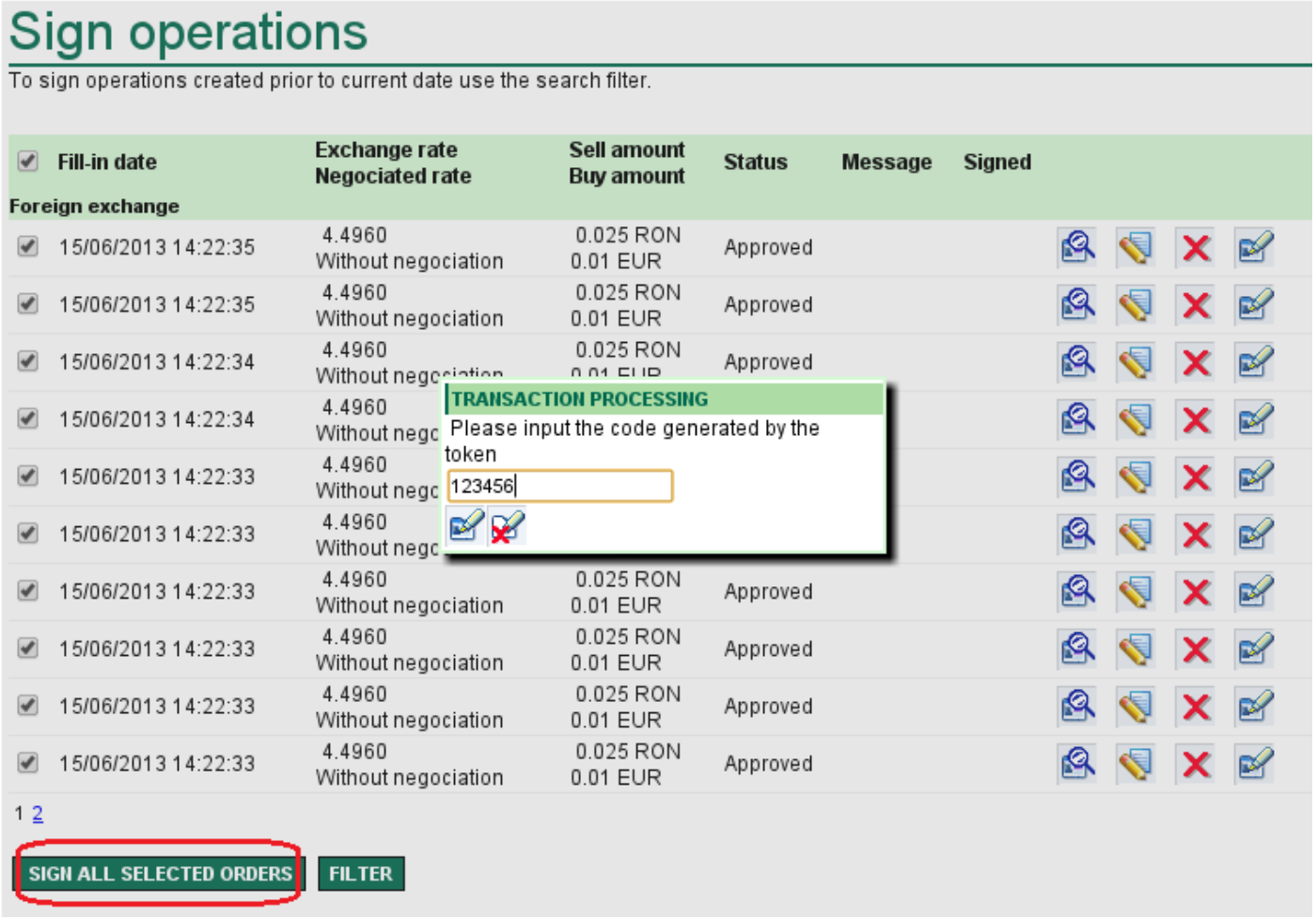
```
POST /ib/Order.aspx?MsgType=MT202&dummy=§1§ HTTP/1.1
Host: [redacted]
Connection: keep-alive
Content-Length: 1056
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Origin: [redacted]
User-Agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.17 (KHTML, like Gecko) Chrome/24.0.1312.70 Safari/537.17
Content-Type: application/x-www-form-urlencoded
Referer: https://[redacted]ib/Order.aspx?MsgType=MT202
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: ASP.NET_SessionId=fkhqrjbalzewxf55s4wuzO2d; __utma=73151883.1110628734.1371293233.1371293233.1371293233.1;
__utmb=73151883.12.10.1371293233; __utmc=73151883; __utmz=73151883.1371293233.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)

ctl00_ScriptManager1_HiddenField=&__EVENTTARGET=ctl00%24Center%24Save&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwUJNzQONjAzOTE2ZBgBBR5fXONvbnR
yb2xzUmVxdW1yZVBvc3RCYWNrS2V5X18WAgUiY3RsMDAkQ2VudGVyJG1zZyROb3RpZnlTdGFOdXNFbWFpbAUfY3RsMDAkQ2VudGVyJG1zZyROZWdvdG1hdGVkUmFOZV6tBuNfxNK
8VRb5UOZTZLTDPM%2BI&__EVENTVALIDATION=%2FwEWFwKth5qrAgKhv5yFAQLx9aHxBgKAktTiCQLEop%2BABwK%2B39TzCQLHu%2FyBDAK9xrfyAgK9xrfyAgK9xrfyAgLHu%
2FyBDALHu%2FyBDALHu%2FyBDAK9xrfyAgKew7eHDAK92fKWAQLO%2FqLPAgLuzbimCAKRqpzxBQLCwa79DwK4%2F67kAQLTyK%2BRCQLKpeLDCErTPFv8DCySyFIsibGX8OLyqd
u2&ctl00%24Center%24msg%24_MsgId=-1&ctl00%24Center%24msg%24_MsgType=MT202&ctl00%24Center%24msg%24OrdName=FURTUNA+CONSTANTIN-ADRIAN&ctl00
%24Center%24msg%24SellAccount=RO78[redacted]021000000136041 2&ctl00%24Center%24msg%24BuyAccount=RO72[redacted]021000000136042 3&ctl00%24Center%24msg%2
4SellAmount=0.025&ctl00%24Center%24msg%24SellCcy=RON&ctl00%24Center%24msg%24BuyAmount=0.01&ctl00%24Center%24msg%24BuyCcy=EUR&ctl00%24Cen
ter%24msg%24FXRate=0.22241992882562277000&ctl00%24ValidationKey=2E3CED13B52A972919B11C7EF6C9B674B1487B5D
```

Add § | Clear § | Auto § | Refresh

Technique 1: Init lots and sign once

- Initiate lots of transactions automatically and sign once



Technique 1: Init lots and sign once

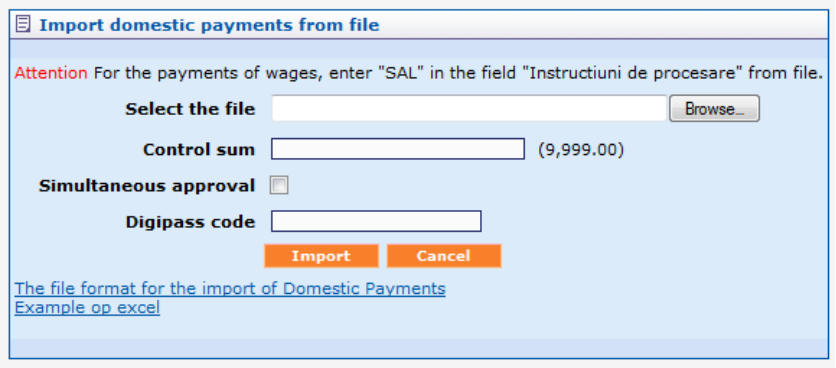
- Initiate lots of transactions automatically and sign once
- Signing can also be automated – stay tuned for next chapter

Technique 2: Payment files

- Upload a payment file containing lots of transactions and sign once

Technique 2: Payment files

- Upload a payment file containing lots of transactions and sign once



	A	B	C	D	E	F	G	H	J	L	N
1	Source Account	Amount	Payment date	Doc ID	Doc Date	Details	Beneficiary Name	Beneficiary Account	Beneficiary Bank	Beneficiary Address	Payment type
2	RO22[redacted]004320117003RO01	0.025	15.06.2013	7182	15.06.2013	payment details	Adrian Furtuna	RO76[redacted]004320117003EU01	Bank XXX	Bucharest	S
3	RO22[redacted]004320117003RO01	0.025	15.06.2013	7182	15.06.2013	payment details	Adrian Furtuna	RO76[redacted]004320117003EU01	Bank XXX	Bucharest	S
4	RO22[redacted]004320117003RO01	0.025	15.06.2013	7182	15.06.2013	payment details	Adrian Furtuna	RO76[redacted]004320117003EU01	Bank XXX	Bucharest	S
5	RO22[redacted]004320117003RO01	0.025	15.06.2013	7182	15.06.2013	payment details	Adrian Furtuna	RO76[redacted]004320117003EU01	Bank XXX	Bucharest	S
6	RO22[redacted]004320117003RO01	0.025	15.06.2013	7182	15.06.2013	payment details	Adrian Furtuna	RO76[redacted]004320117003EU01	Bank XXX	Bucharest	S
7	RO22[redacted]004320117003RO01	0.025	15.06.2013	7182	15.06.2013	payment details	Adrian Furtuna	RO76[redacted]004320117003EU01	Bank XXX	Bucharest	S
8	RO22[redacted]004320117003RO01	0.025	15.06.2013	7182	15.06.2013	payment details	Adrian Furtuna	RO76[redacted]004320117003EU01	Bank XXX	Bucharest	S
9	RO22[redacted]004320117003RO01	0.025	15.06.2013	7182	15.06.2013	payment details	Adrian Furtuna	RO76[redacted]004320117003EU01	Bank XXX	Bucharest	S
10	RO22[redacted]004320117003RO01	0.025	15.06.2013	7182	15.06.2013	payment details	Adrian Furtuna	RO76[redacted]004320117003EU01	Bank XXX	Bucharest	S
11	RO22[redacted]004320117003RO01	0.025	15.06.2013	7182	15.06.2013	payment details	Adrian Furtuna	RO76[redacted]004320117003EU01	Bank XXX	Bucharest	S
12	RO22[redacted]004320117003RO01	0.025	15.06.2013	7182	15.06.2013	payment details	Adrian Furtuna	RO76[redacted]004320117003EU01	Bank XXX	Bucharest	S

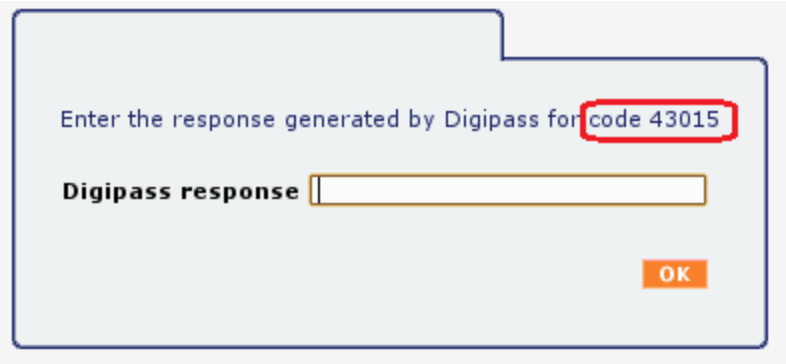
- Signing can also be automated – stay tuned for next chapter

Technique 3: Real time transactions + rainbow tables

- Do real time transactions automatically and sign using pre-computed digipass responses

Technique 3: Real time transactions + rainbow tables

- Do real time transactions automatically and sign using pre-computed digipass responses
- Applicable when signing is done using challenge-response mechanism, with challenge code <= 5 digits



Technique 3: Real time transactions + rainbow tables

- A challenge-response digipass returns the same response for the same challenge code every time

```
Response   = f(challenge, timestamp, client ID, other data)
           = f(challenge, static data)
```

- Build rainbow tables with digipass responses
  - Feasible for max 5 digit challenge codes
  - Max 99999 possibilities
  - Can be automated, stay tuned

Technique 4: Real time transactions + digipass automation

- Do real time transactions automatically and sign using digipass responses computed in real time

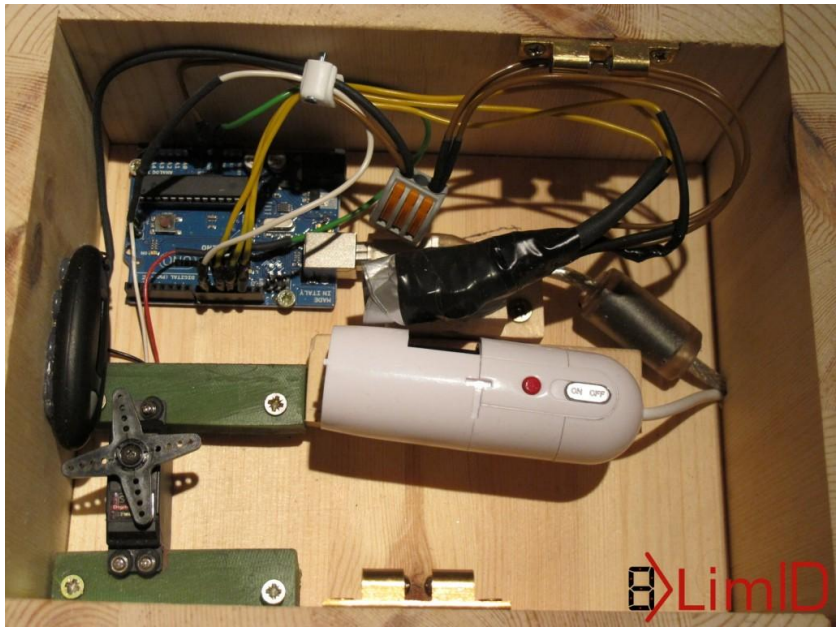
Technique 4: Real time transactions + digipass automation

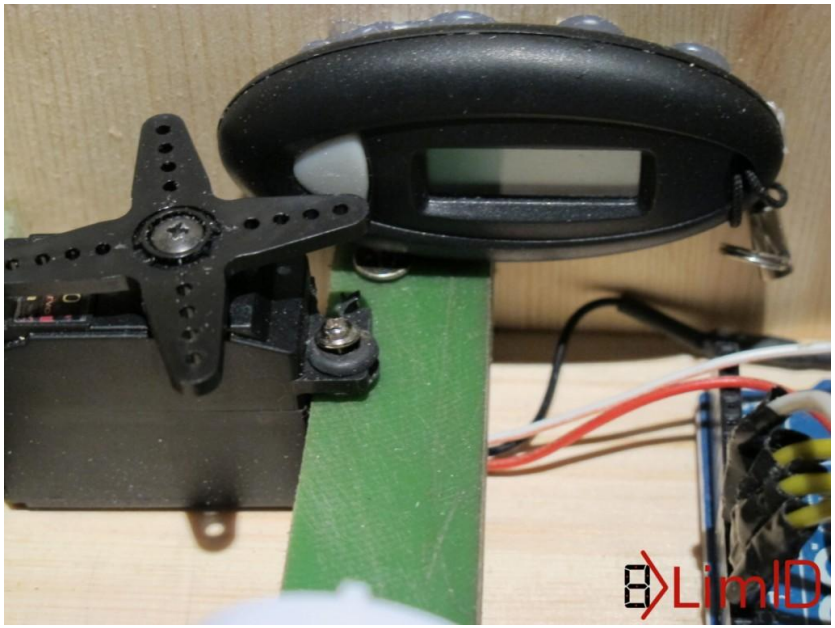
- Do real time transactions automatically and sign using digipass responses computed in real time
- Requires automation of the signing device (digipass, phone, etc)

Digipass automation

LimID project (for VASCO GO3)

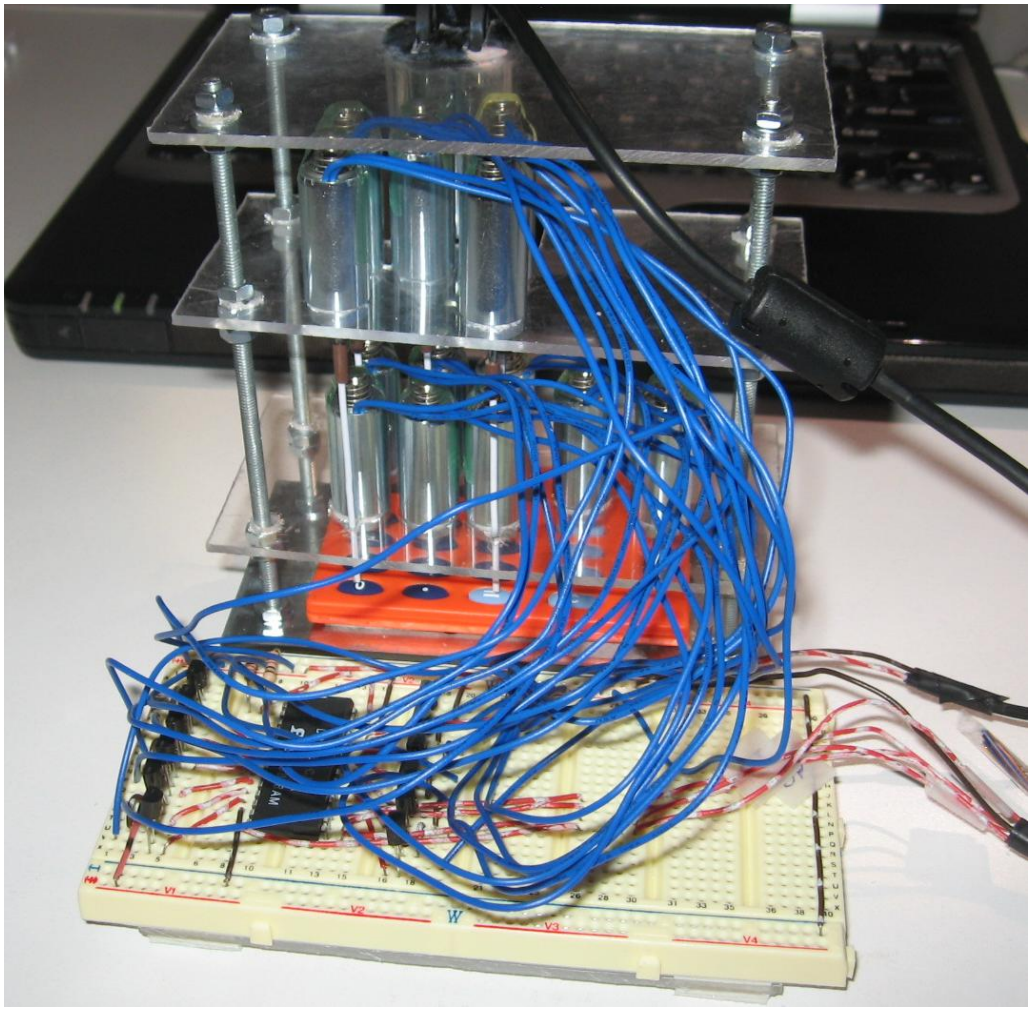
- http://limid.sitadella.com
- Code regenerates at 30 seconds





- Video

My machine (for VASCO 550)



Requires PIN authentication

Used for:

- 2nd factor authentication
- Transaction signing

My machine - video

My machine - current performance

- 10 transactions / minute (1 transaction / 6 seconds)
  - max 14400 transactions / day
  - enter PIN, type challenge code, read response image, do OCR
- Our previous example:

  100 RON → 190 RON (gain ~20 EUR)

  => 4347 transactions * 6 sec/trans = **26082 sec**

  = 7h:14m:42 s
- Maximum amount to multiply per day:

  14400 * 0.023 RON = 331.2 RON => final 629.28 RON

  gain 298 RON ~= 68 EUR/day

My machine - current performance

- 10 transactions / minute (1 transaction / 6 seconds)
  - max 14400 transactions / day
  - enter PIN, type challenge code, read response image, do OCR
- Our previous example:

  100 RON → 190 RON (gain ~20 EUR)

  => 4347 transactions * 6 sec/trans = **26082 sec**

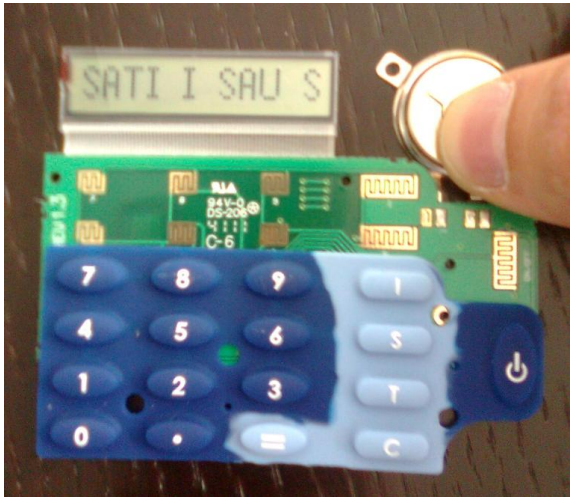
  = 7h:14m:42 s
- Maximum amount to multiply per day:

  14400 * 0.023 RON = 331.2 RON => final 629.28 RON

  gain 298 RON ~= 68 EUR/day
- What about doing in parallel (on multiple bank accounts)?
- Money making machine? ☺

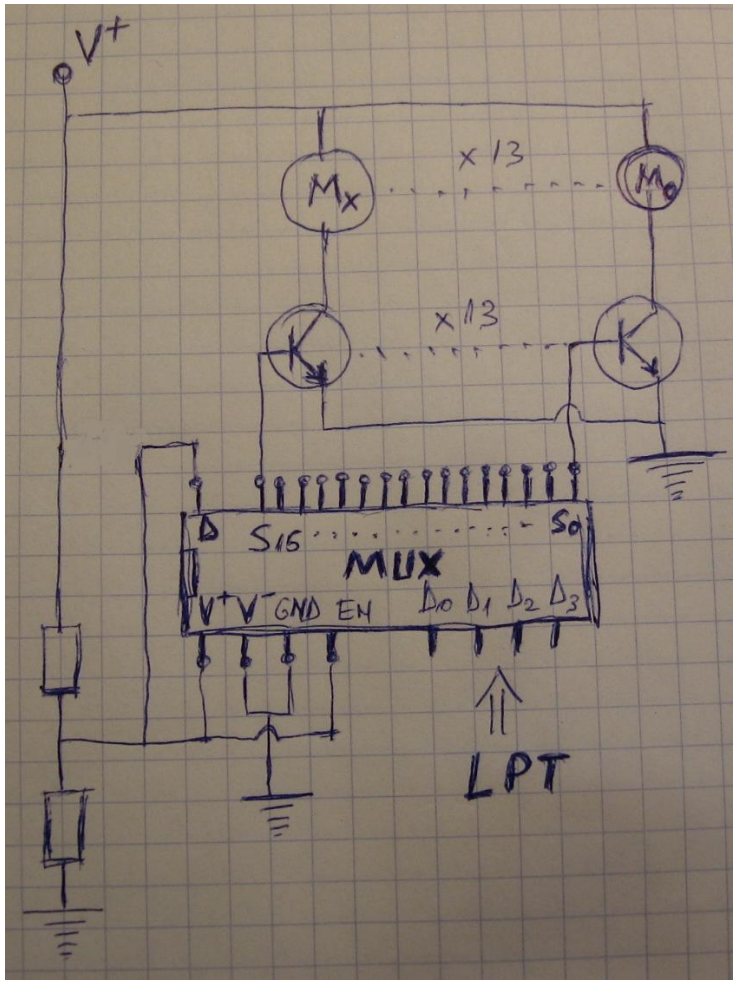
External vs Internal instrumentation

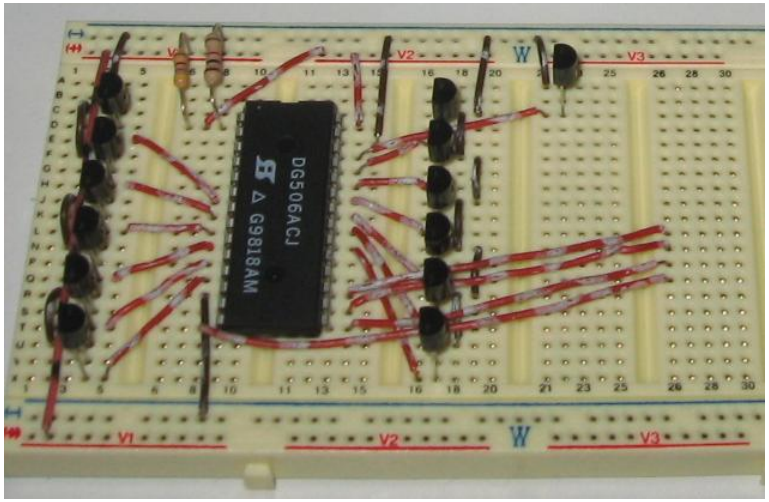
- Internal instrumentation (direct electrical connections):
  - Pros:
    - more reliable and faster
    - almost error free
  - Cons:
    - might not be possible – some digipasses deactivate when opened
    - must know the pinout of LCD screen (lots of pins!)
    - sensitive soldering required
    - mistakes can lead to deactivation

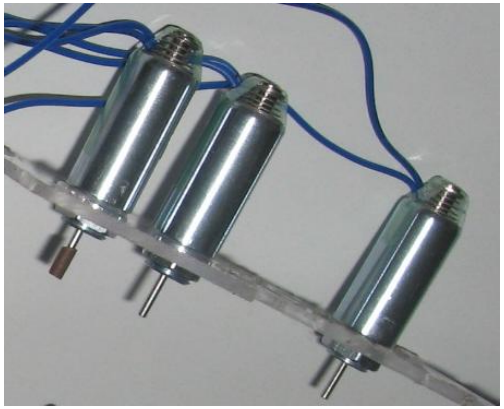


- External instrumentation:
  - Pros:
    - No interference with digipass's internals
    - Can be applied to any digipass model
  - Cons:
    - Pretty slow (but good for the "low and slow" approach)
    - Some (mechanics) errors occur on pressing buttons (resolvable by a more professional construction)
    - OCR process needs special (lighting) conditions to produce correct results

My machine – implementation details (1)

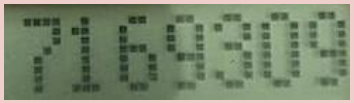
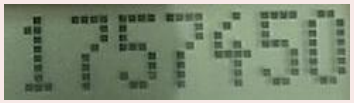
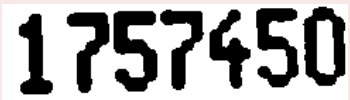
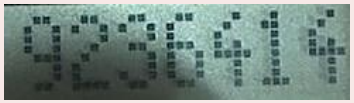




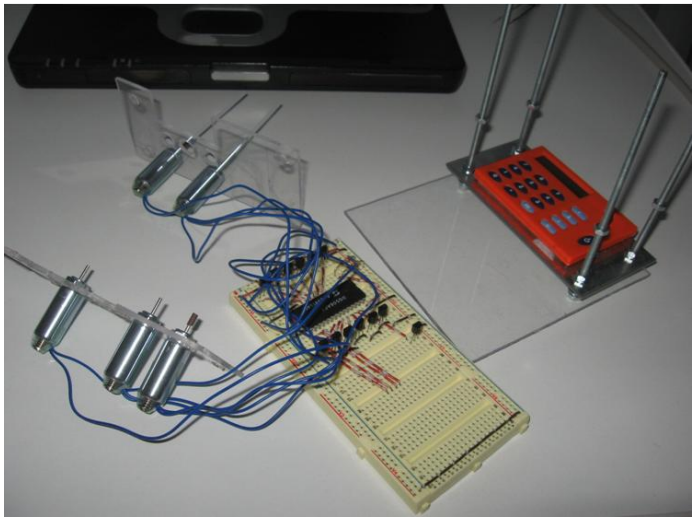


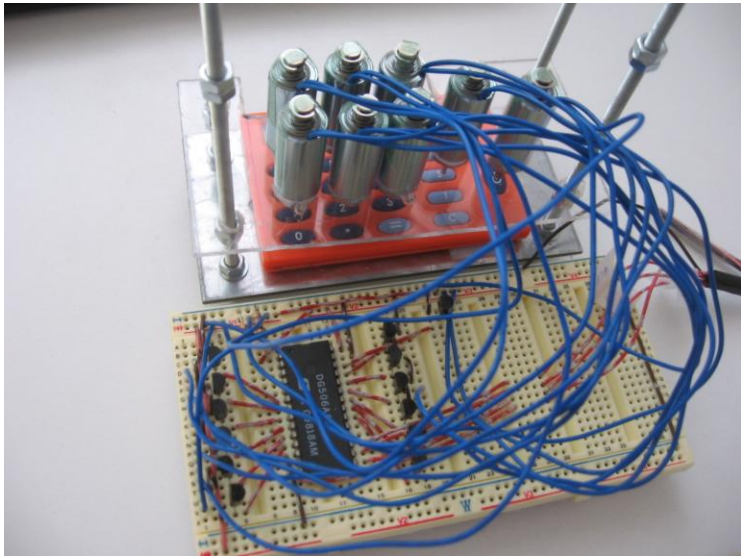
My machine – implementation details (2)

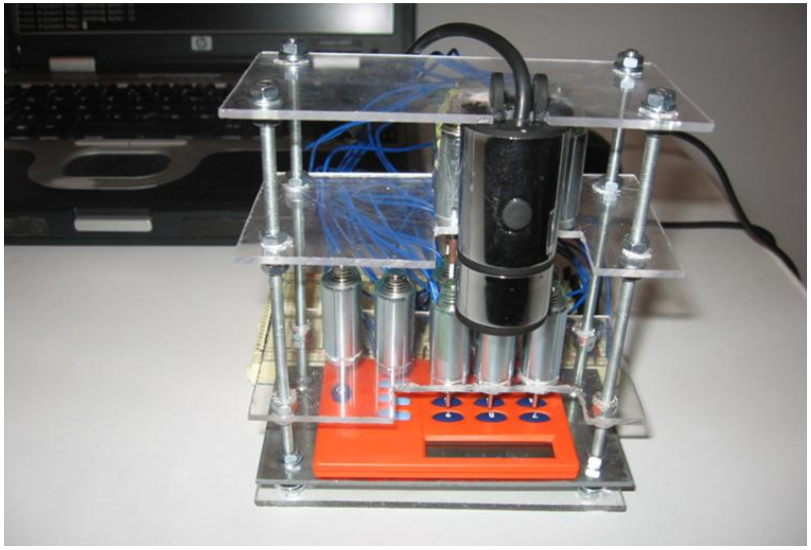
Optical Character Recognition

Original	Cleared background	Blurred	Threshold applied	OCR-ized gocr / ocrad
				7169309 -_16g309
				1757450 1_5_G50
				043i __ i_ì OG3i _i_i
				9a__641 4 9__6G1G

My machine – development stages







Live Demo

Q & A

Thank you!

Adrian Furtunã, PhD, OSCP, CEH
adif2k8@gmail.com
http://pentest-tools.com