

# Breaking e-Banking CAPTCHAs

Shujun Li<sup>1</sup>, Syed Amier Haider Shah<sup>2</sup>, Muhammad Asad  
Usman Khan<sup>2</sup>, Syed Ali Khayam<sup>2</sup>, Ahmad-Reza Sadeghi<sup>3</sup>,  
Roland Schmitz<sup>4</sup>

<sup>1</sup>Zukunftskolleg, University of Konstanz, Germany

<sup>2</sup>National University of Science and Technology, Pakistan

<sup>3</sup>Ruhr-University of Bochum, Germany

<sup>4</sup>Stuttgart Media University, Germany

# Outlines

- Our motivation
  - e-banking security is important
  - CAPTCHAs are widely used in e-banking systems
- Our subjects of study
  - 44 e-banking CAPTCHA schemes
  - $O(10^3)$  financial institutions +  $O(10^8)$  customers
- Our findings
  - All e-banking CAPTCHAs were broken with a carefully selected set of CAPTCHA-breaking tools.
  - CAPTCHA does NOT seem to be a sufficient e-banking security solution.

# Traditional CAPTCHAs: Preventing automated login/logon

- CAPTCHAs against web bots
  - **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part



I am a human!



Then solve this!



Type the characters you see in the picture below.

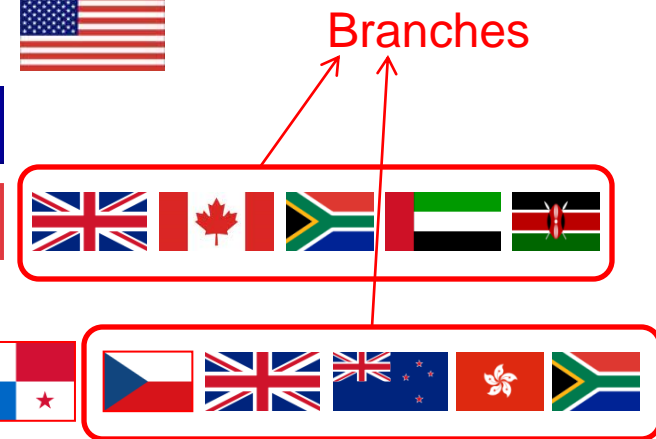
*dëricak*

Letters are not case-sensitive

# e-banking CAPTCHAs everywhere?

## - Login CAPTCHAs: 41 schemes

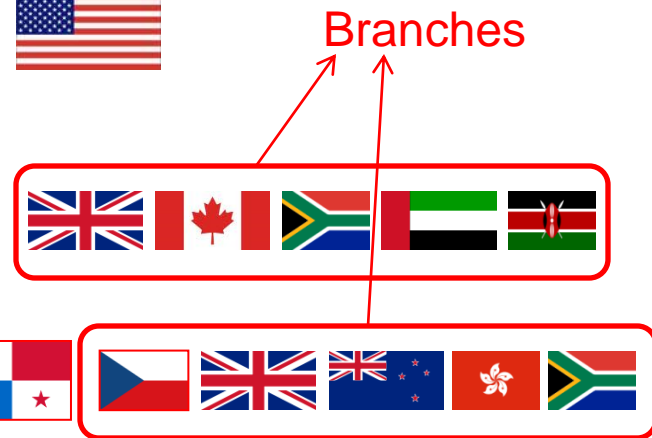
- Most banks in China  O(100) million customers
- O(100) banks in Germany 
- O(1000) financial institutions in USA 
- Four credit unions in Australia 
- One major bank in Switzerland 
- One bank in Pakistan 
- One bank in Central America 




# e-banking CAPTCHAs everywhere?

## - Login CAPTCHAs: 41 schemes

- Most banks in China   $O(100)$  million customers
- $O(100)$  banks in Germany 
- $O(1000)$  financial institutions in USA 
- Four credit unions in Australia 
- One major bank in Switzerland 
- One bank in Pakistan 
- One bank in Central America 



## - Transaction CAPTCHAs: 3 schemes

- 2 schemes @ two major banks in China 
  - 1 scheme @  $O(100)$  banks in Germany 
- > 110 million customers

# What are transaction CAPTCHAs?

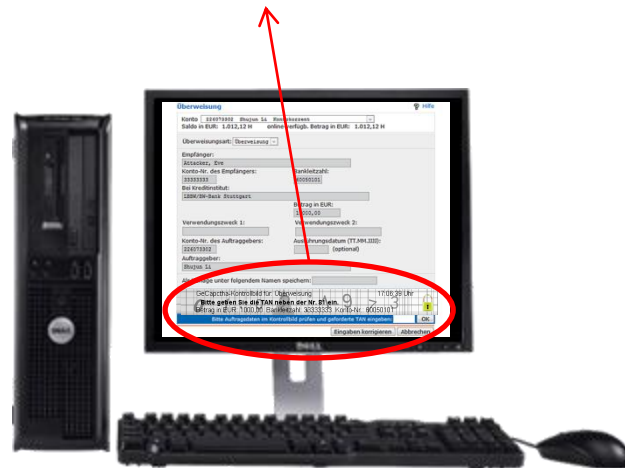
- GeCaptcha as a typical example
  - GeCaptcha is the transaction e-banking CAPTCHA scheme currently used by  $O(100)$  German banks.



I want to transfer money!

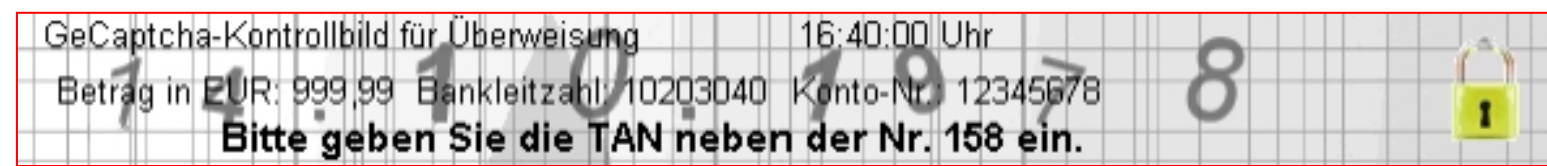


Then solve this!

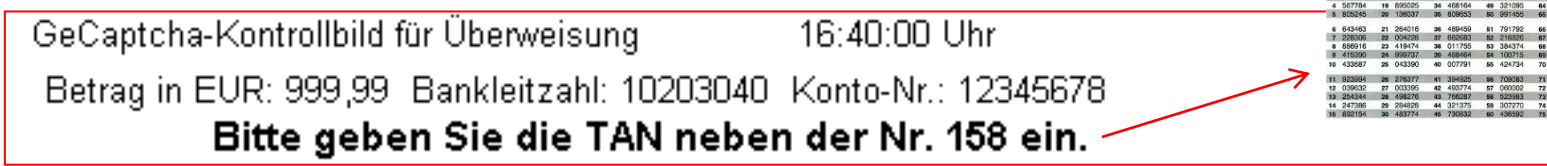


# What are transaction CAPTCHAs?

## - An anatomy of GeCaptcha



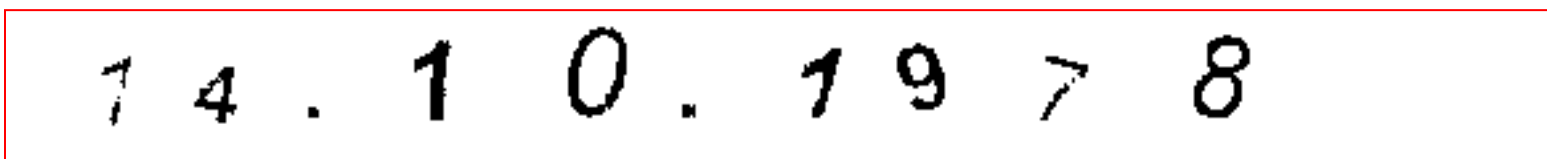
=



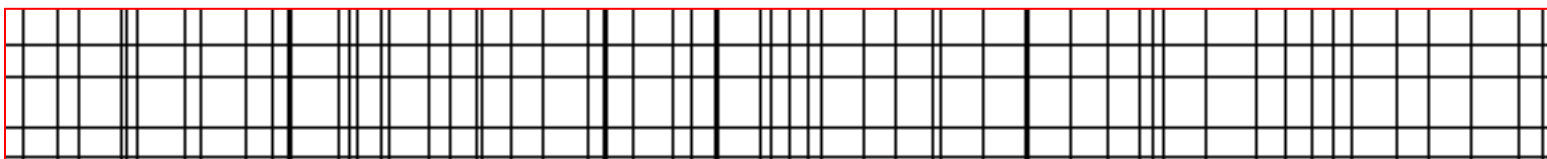
- Bitte die TAN-Liste nicht zerschneiden -

1	548300	16	700592	31	087520	46	561281	61	007963	76	715077	91	395055
2	444338	17	150583	32	557713	47	646705	62	121148	77	469371	92	781128
3	121038	18	054071	33	538881	48	549384	63	458195	78	243337	93	496726
4	267734	19	695225	34	458164	49	371305	64	154380	79	201360	94	513333
5	832545	20	136037	35	830653	50	991405	65	755945	80	111540	95	385665
6	043463	21	254516	36	489400	51	791782	66	036473	81	424055	96	801881
7	038596	22	004506	37	883283	52	718802	67	169193	82	361823	97	368828
8	413390	23	419474	38	011755	53	354374	68	275525	83	382473	98	213656
9	433687	24	566932	39	489464	54	130716	69	903097	84	384303	99	444205
10	433687	25	413390	40	007791	55	424734	70	522588	85	291127	100	385674
11	022889	26	278077	41	384628	56	730643	71	565747	86	794324	101	546885
12	038032	27	020356	42	493774	57	700302	72	591349	87	702747	102	753403
13	254344	28	498276	43	746287	58	523983	73	896203	88	179774	103	154258
14	247385	29	254628	44	121375	59	207273	74	030443	89	532040	104	252579
15	882154	30	482774	45	730632	60	136582	75	591411	90	903282	105	859138

+



+



# How does a real attack work?

- Scene 1: I try to transfer 10 EUR to Bob.

**Überweisung** [Hilfe](#)

Konto: 226073302 Shujun Li Kontokorrent [Auswählen](#)

Saldo in EUR: 1.012,12 H online-verfügb. Betrag in EUR: 1.012,12 H

Überweisungsart: Überweisung [Ändern](#)

Empfänger: Friend, Bob [Aus Vorlage](#)

Konto-Nr. des Empfängers: 111111111 Bankleitzahl: 69291000 [BLZ suchen](#)

Bei Kreditinstitut: Wird automatisch gefüllt

Betrag in EUR: 10

Verwendungszweck 1: Verwendungszweck 2: [Mehr](#)

Konto-Nr. des Auftraggebers: 226073302 Ausführungsdatum (TT.MM.JJJJ): (optional)

Auftraggeber: Shujun Li

Als Vorlage unter folgendem Namen speichern:

[Eingaben prüfen](#) [Eingaben löschen](#)

Receiver's name

Receiver's  
account number

Bank code

Amount  
in EUR



# How does a real attack work?

- Scene 2: Eve's Trojan manipulates transaction data.

**Überweisung** [Hilfe](#)

Konto:    
 Saldo in EUR: 1.012,12 H online-verfügb. Betrag in EUR: 1.012,12 H

Überweisungsart:

Empfänger:  
~~Friend, Bob~~ **Attacker, Eve**

Konto-Nr. des Empfängers:  
~~111111111~~ **33333333**

Bankleitzahl:  
~~11111111~~ **60050101**

Bei Kreditinstitut:  
 Wird automatisch gefüllt

Betrag in EUR:  
~~1000~~ **1000**

Verwendungszweck 1:   
 Verwendungszweck 2:

Konto-Nr. des Auftraggebers:

Ausführungsdatum (TT.MM.JJJJ):  
 (optional)

Auftraggeber:

Als Vorlage unter folgendem Namen speichern:

# How does a real attack work?

- Scene 3: Sever sends a GeCaptcha image back.

**Überweisung** [Hilfe](#)

Konto    
 Saldo in EUR: 1.012,12 H online-verfügb. Betrag in EUR: 1.012,12 H

Überweisungsart:

Empfänger:    
 Konto-Nr. des Empfängers:  Bankleitzahl:    
 Bei Kreditinstitut:    
 Betrag in EUR:    
 Verwendungszweck 1:  Verwendungszweck 2:    
 Konto-Nr. des Auftraggebers:  Ausführungsdatum (TT.MM.JJJJ):  (optional)   
 Auftraggeber:    
 Als Vorlage unter folgendem Namen speichern:

GeCaptcha-Kontrollbild für: Überweisung 17:06:39 Uhr   
**Bitte geben Sie die TAN neben der Nr. 81 ein.**   
 Betrag in EUR: 1000,00 Bankleitzahl: 33333333 Konto-Nr.: 60050101   
 Bitte Auftragsdaten im Kontrollbild prüfen und geforderte TAN eingeben:

# How does a real attack work?

- Scene 4: Eve's Trojan forges a GeCaptcha image.

**Überweisung** [Hilfe](#)

Konto: 226073302 Shujun Li Kontokorrent  
Saldo in EUR: 1.012,12 H online-verfügb. Betrag in EUR: 1.012,12 H

Überweisungsart: Überweisung

Empfänger:  
Friend, Bob  
Konto-Nr. des Empfängers: 1111111111 Bankleitzahl: 69291000  
Bei Kreditinstitut: Volksbank Konstanz

Betrag in EUR: 10,00

Verwendungszweck 1:  
Verwendungszweck 2:

Konto-Nr. des Auftraggebers: 226073302  
Ausführungsdatum (TT.MM.JJJJ): (optional)

Auftraggeber: Shujun Li

Als Vorlage unter folgendem Namen speichern:

Betrag in EUR: 10,00 Bankleitzahl: 1111111111 Konto-Nr.: 69291000

**Bitte geben Sie die TAN neben der Nr. 81 ein.**  
GeCaptcha-Kontrollbild für: Überweisung 10:53:05 Uhr

Bitte Auftragsdaten im Kontrollbild prüfen und geforderte TAN eingeben:

# How does a real attack work?

- Scene 5: I find the TAN No. 81 in my indexed TAN list and send it (424005) to Eve's Trojan.

- Bitte die iTAN-Liste nicht zerschneiden -

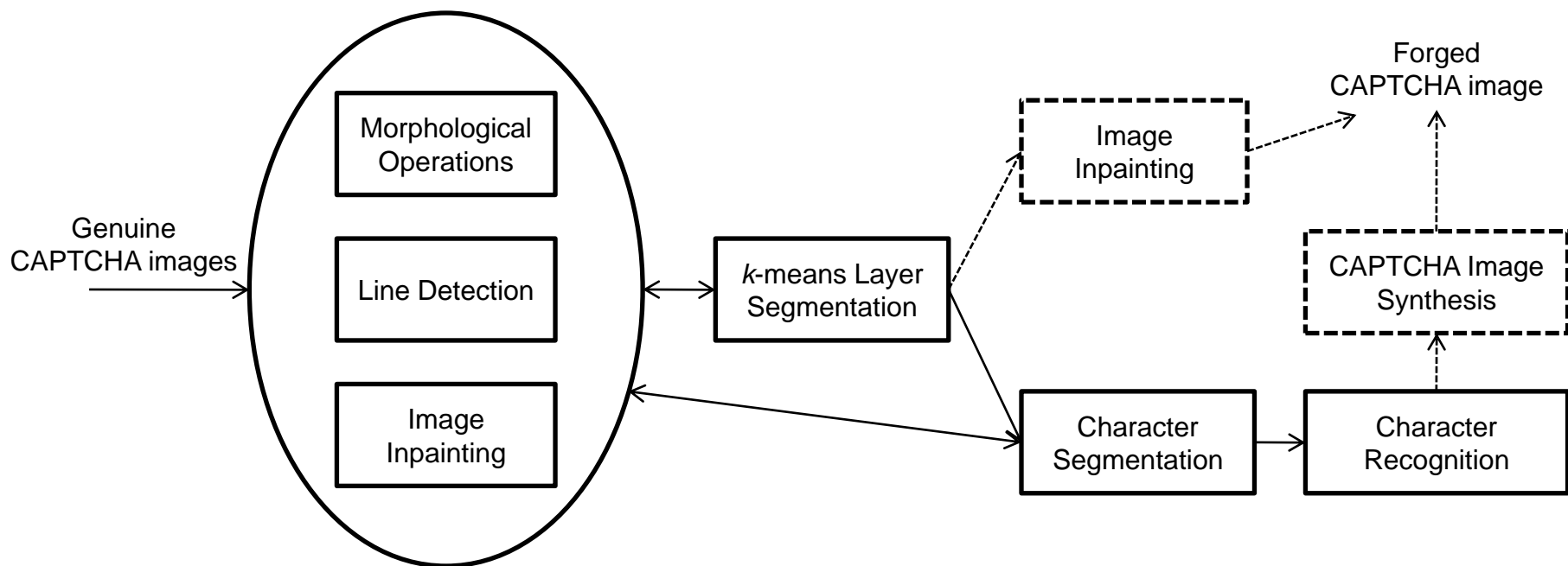
1	643103	16	760882	31	361750	46	561231	61	027663	76	719377	91	995550
2	444098	17	150983	32	557718	47	646765	62	120148	77	469971	92	761108
3	121038	18	094071	33	528881	48	549388	63	456195	78	245337	93	696726
4	567784	19	895025	34	468164	49	321095	64	154386	79	269366	94	515383
5	805245	20	138037	35	809553	50	991455	65	755948	80	111545	95	985669
6	643463	21	264016	36	489459	51	791792	66	036473	81	424005	96	908881
7	228306	22	004226	37	662683	52	216826	67	195913	82	227066	97	959823
8	886916	23	419474	38	011755	53	384374	68	275525	83	380473	98	219656
9	415390	24	999737	39	468464	54	100715	69	903557	84	884352	99	446325
10	433687	25	043390	40	007791	55	424734	70	822588	85	291127	100	388574
11	923994	26	276377	41	384925	56	709083	71	669747	86	794354	101	646695
12	039632	27	003395	42	493774	57	060002	72	291949	87	762747	102	792483
13	254344	28	498276	43	766287	58	523583	73	695203	88	179774	103	154218
14	247386	29	294826	44	321375	59	907270	74	039343	89	535240	104	356379
15	892154	30	483774	45	730832	60	436592	75	591411	90	900286	105	859196

- Scene 6: Eve's Trojan sends 424005 to the server.
- Scene 7: The server validates the received TAN and accepts the **manipulated** transaction request.
- Scene 8: (Some days/weeks later) I realized that my money had been stolen.

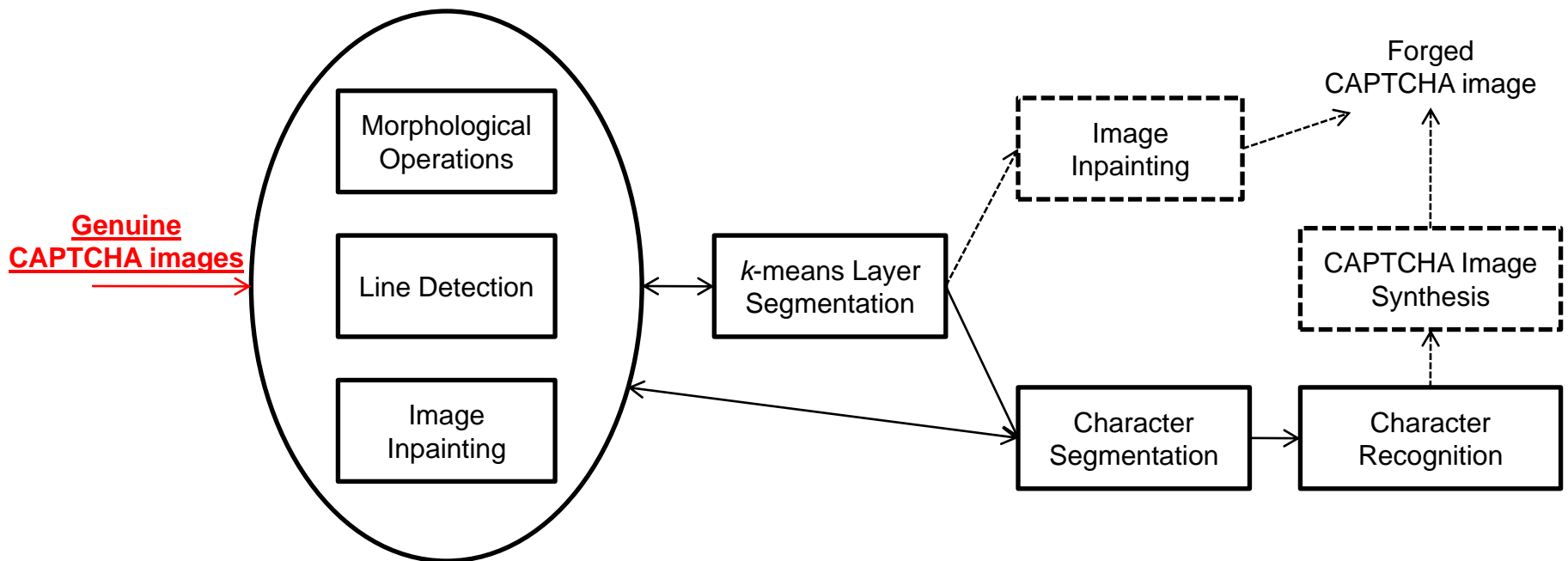
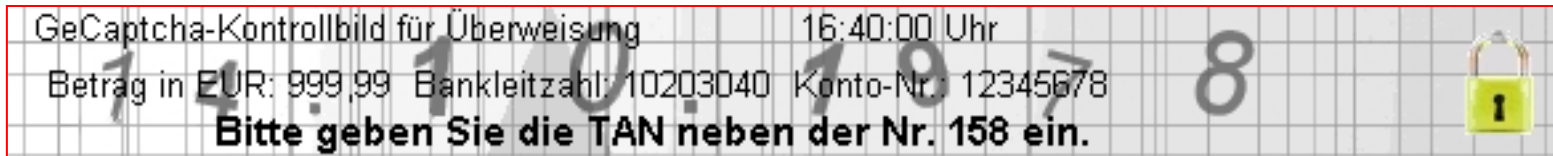
# How to forge a GeCaptcha image?

## A CAPTCHA-breaking network

- Image processing + Pattern recognition

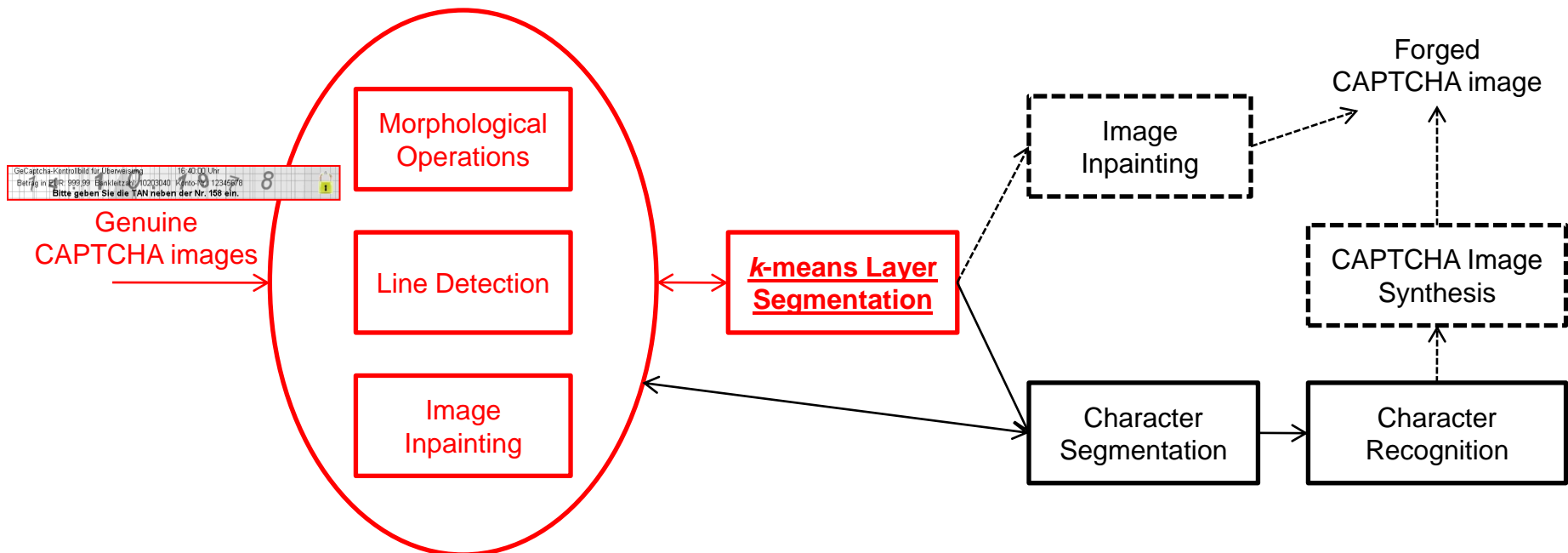


# How to forge a GeCaptcha image? Automated Attack 1



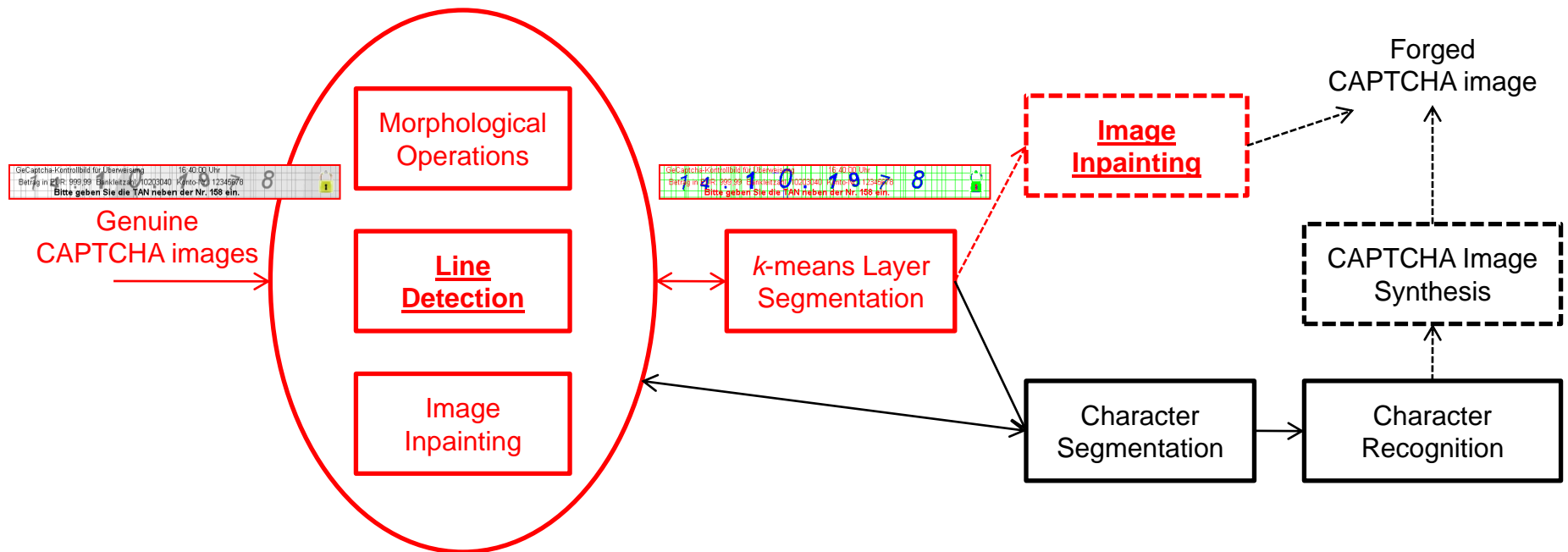
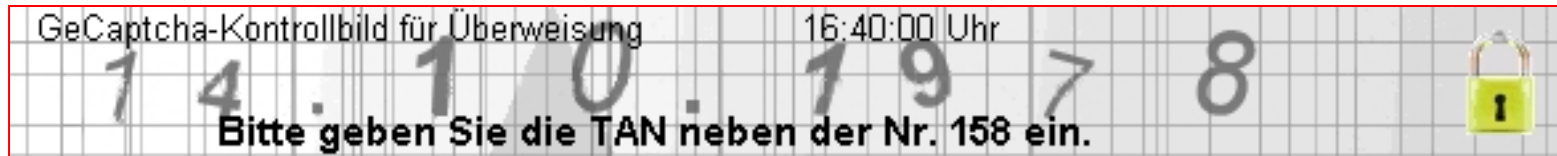
# How to forge a GeCaptcha image?

## Automated Attack 1



# How to forge a GeCaptcha image?

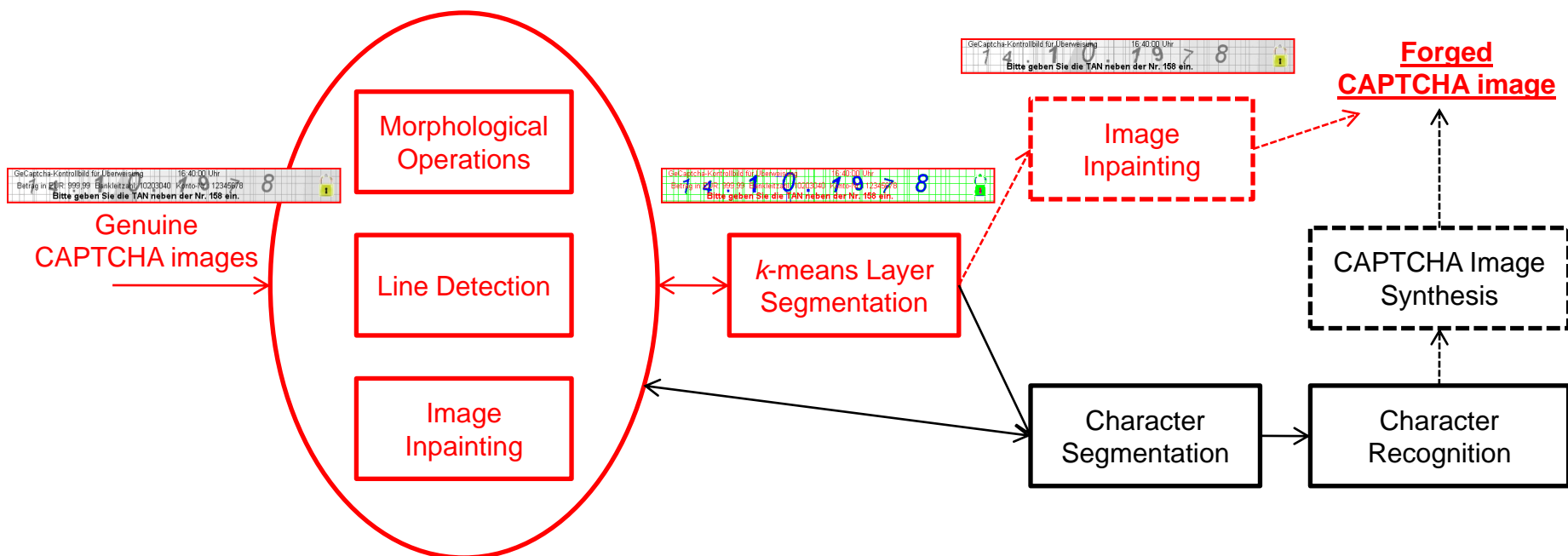
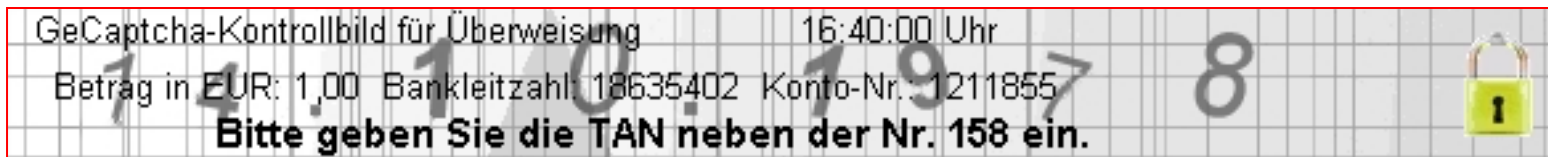
## Automated Attack 1





# How to forge a GeCaptcha image?

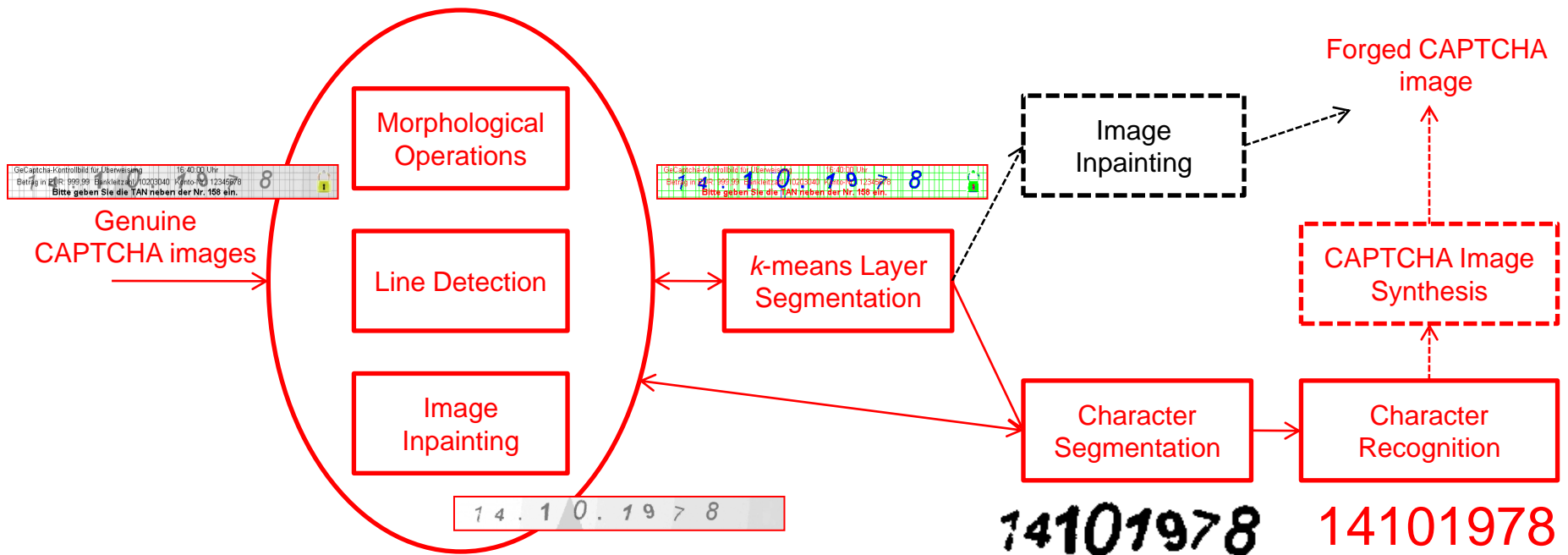
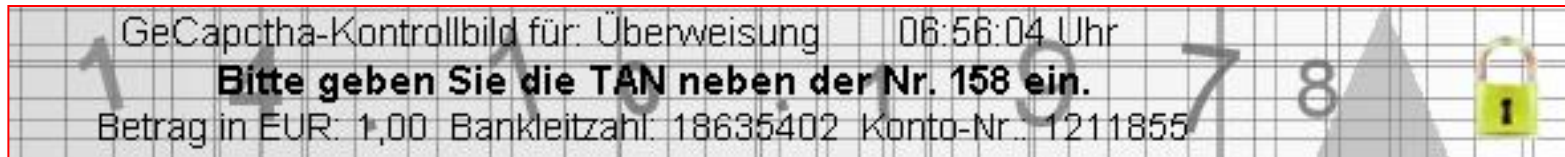
## Automated Attack 1



**Successful rate = 100/100=100%**

# How to forge a GeCaptcha image?

## Automated Attack 2






**Successful rate = 100/100=100%**

# Breaking GeCaptcha: Efficiency of the attacks

- Automated Attack 1
  - Average running time  $\approx 250$  ms
- Automated Attack 2
  - Stage 1 (offline): Average running time  $\approx 5$  seconds
  - Stage 2 (online): Average running time  $\approx 190$  ms
- Platform
  - Software: MATLAB 2008b / 2010a / 2010b
  - Hardware: Levono ThinkPad T61 laptop with an Intel Core2 Duo 2.4 GHz CPU and with 2 GB memory

# Go beyond GeCaptcha: All e-banking CAPTCHAs broken!

- 3 transaction e-banking CAPTCHA schemes

-  GeCaptcha: 100/100=100%
-  ChCaptcha1: 100/100=100%
-  ChCaptcha2: 103/103=100%

- 41 login e-banking CAPTCHA schemes

- 38 schemes:  $n/n=100\%$
- 3 schemes:  $m/n>95\%$

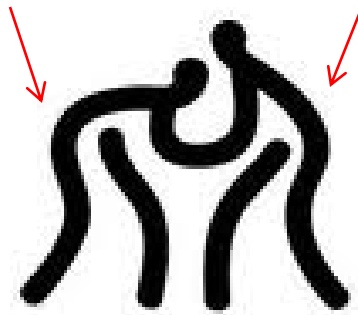


- Here,  $n \geq 60$



# e-banking CAPTCHAs: Love them or leave them?

- e-banking CAPTCHAs cannot be easily enhanced.
- Strong CAPTCHAs are hard to define and design.
- A more critical security-usability tradeoff



- Banks are passive and always want to save costs.
- Our recommendations
  - Stopping depending on e-banking CAPTCHAs!
  - Moving to trusted hardware!



# Thanks for your attention!

## Now it's time for questions 😊

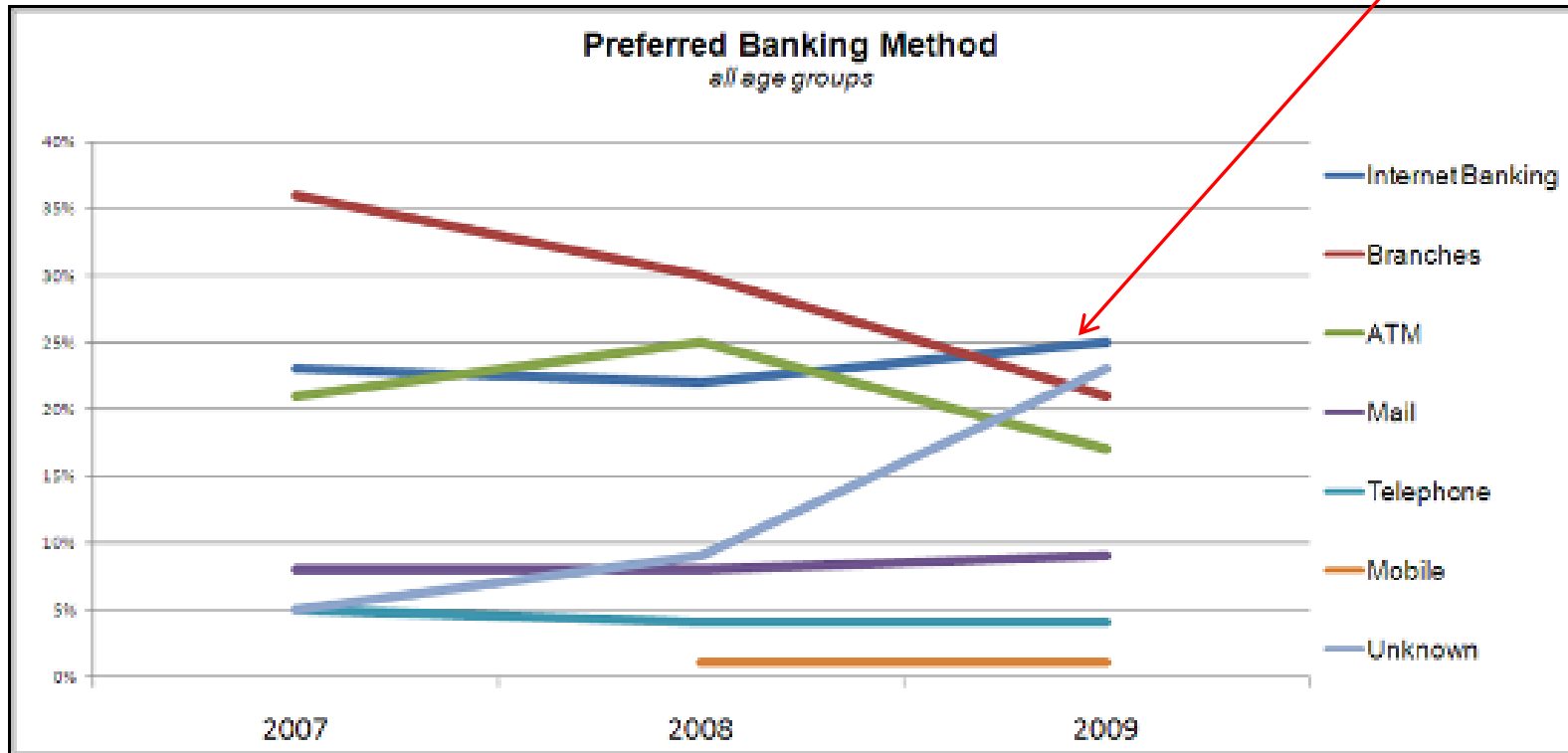


Find more at <http://www.hooklee.com/default.asp?t=eBankingCAPTCHAs>

# e-banking: Bank customer's first choice now!

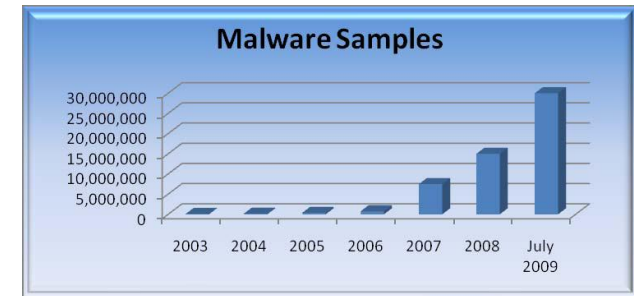
-  American Bankers Association survey (2009)

**Internet Banking**



# Is e-banking indeed secure?

- We are living in an insecure cyberworld ☹



- A CS student of Uni-Konstanz said:
  - "I don't use e-banking. I am lazy and afraid of ..."



# e-banking security measures

- A list of e-banking security measures against different threats (phishing, MiTM, malware, etc.):

- login CAPTCHAs
- indexed TAN
- transaction CAPTCHAs

Anmeldung Banking-Portal

Kundennummer

Online-PIN

Zugriffscode **284567**

Bitte die TAN-Liste nicht anschauen!

1	643103	16	700990	31	597755	46	261231	61	007963	76	719277	91	999920
2	444098	17	150563	32	557718	47	646765	62	120148	77	469271	92	761108
3	121036	18	896971	33	326681	48	246886	63	091186	78	266337	93	899776
4	567794	19	895025	34	408164	49	321086	64	154386	79	603305	94	510383
5	805245	20	136587	35	809553	50	991905	65	759995	80	111545	95	355989
6	643463	21	254016	36	489459	51	791792	66	034473	81	424005	96	905881
7	288506	22	004258	37	433053	52	216826	67	109293	82	029666	97	355823
8	888918	23	419474	38	011755	53	384374	68	275325	83	384373	98	219656
9	410390	24	989737	39	988484	54	100715	69	063337	84	384362	99	440325
10	433687	25	043360	40	007791	55	424734	70	622588	85	291127	100	368674
11	923894	26	276377	41	354825	56	700083	71	569747	86	794354	101	549695
12	036032	27	033195	42	403774	57	000302	72	291843	87	762717	102	724403
13	254344	28	498276	43	766287	58	523983	73	693303	88	179774	103	154218
14	247380	29	294529	44	321375	59	307270	74	008343	89	533540	104	355379
15	826254	30	489774	45	700382	60	456962	75	581611	90	300266	105	359195

GeCaptcha-Kontrollbild für Überweisung 16:40:00 Uhr  
Betrag in EUR: 999.99 Bankleitzahl: 10203040 Konto-Nr. 12345678  
Bitte geben Sie die TAN neben der Nr. 158 ein.

收款账号: 800167645271613670  
收款人: 冯七  
验证码: 请输入账号中红色大号字体的数字

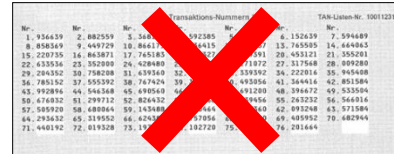
显示! 请认真核对以下信息:  
转入账号: 440209000618392  
转入账号名称: 张三  
转账金额: 100.00

- mobile TAN
- hardware TAN generators
- photoTAN
- HBCI/FinTS
- ...



# e-banking security and usability: other measures deployed by banks

- indexed TAN
  - Not secure against MitM attack
- mobile TAN
  - Not secure against mobile malware
  - Out-of-band channel does not exist for mobile banking
  - Additional costs (SMS)
  - Untrusted telecommunication service provider
- photoTAN
  - Not secure against mobile malware
- hardware TAN generators and smart card readers
  - Not very portable (usable), not cheap (no free lunch, > 10 €)
  - But it seems to be the only way to go for the long run.



# What did we use for breaking e-banking CAPTCHAs?

- Two **new** tools
  - Digital image inpainting



- Image quality assessment (IQA) for character recognition:  
CW-SSIM = **C**omplex **W**avelet **S**tructural **S**imilarity **M**etric

standard templates



sample test images (randomly selected from 2430 images)



# How to forge a GeCaptcha image?

## Automated Attack 1

- Step 0: Segment the GeCaptcha image
- Step 1: Locate the text line with transaction data
- Step 2: Remove the genuine transaction data
- Step 3: Add user-expected transaction data



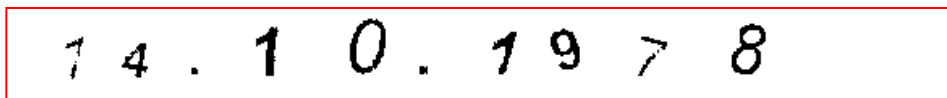
Betrag in EUR: 999,99 Bankleitzahl: 10203040 Konto-Nr.: 12345678



# How to forge a GeCaptcha image?

## Automated Attack 2

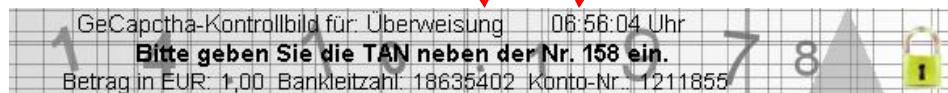
- Stage 1 (offline): Recognize the user's birthday
- Stage 2 (online): Forge GeCaptcha images



14101978

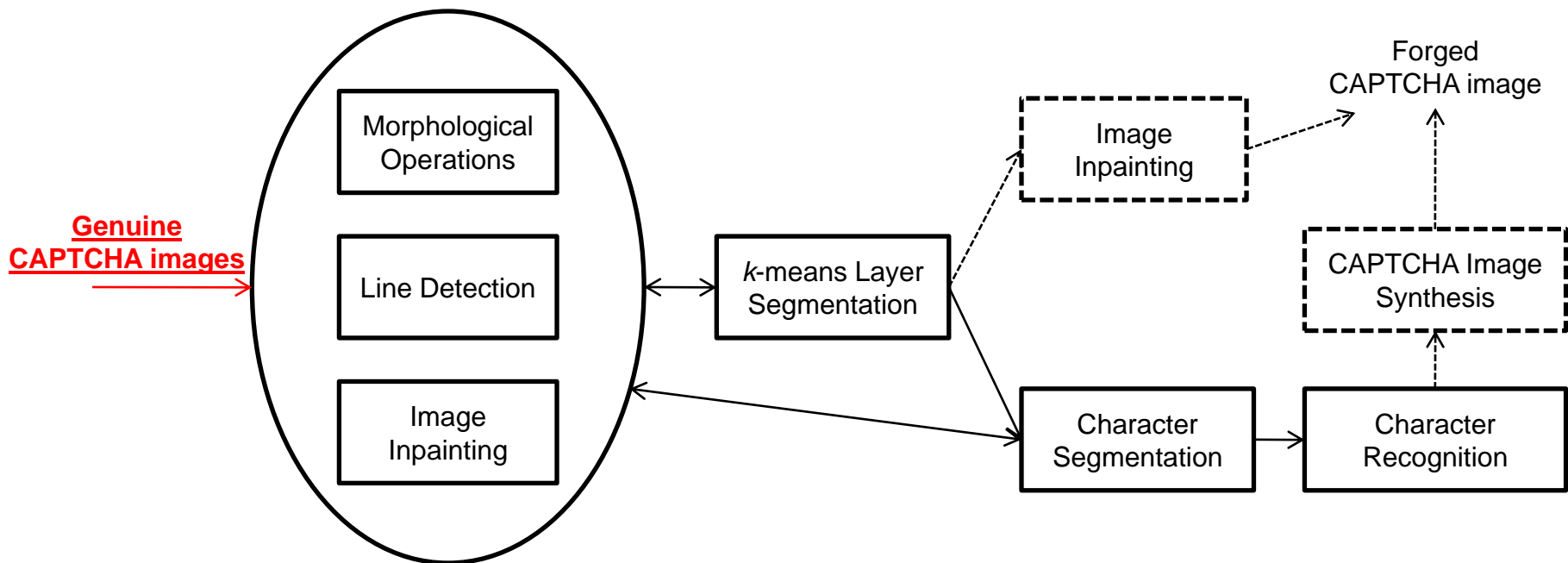
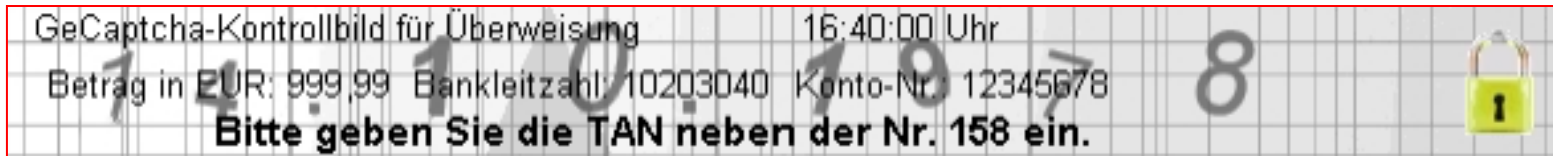
14 10 1978 ✓

Bitte geben Sie die TAN neben der Nr. 158 ein.



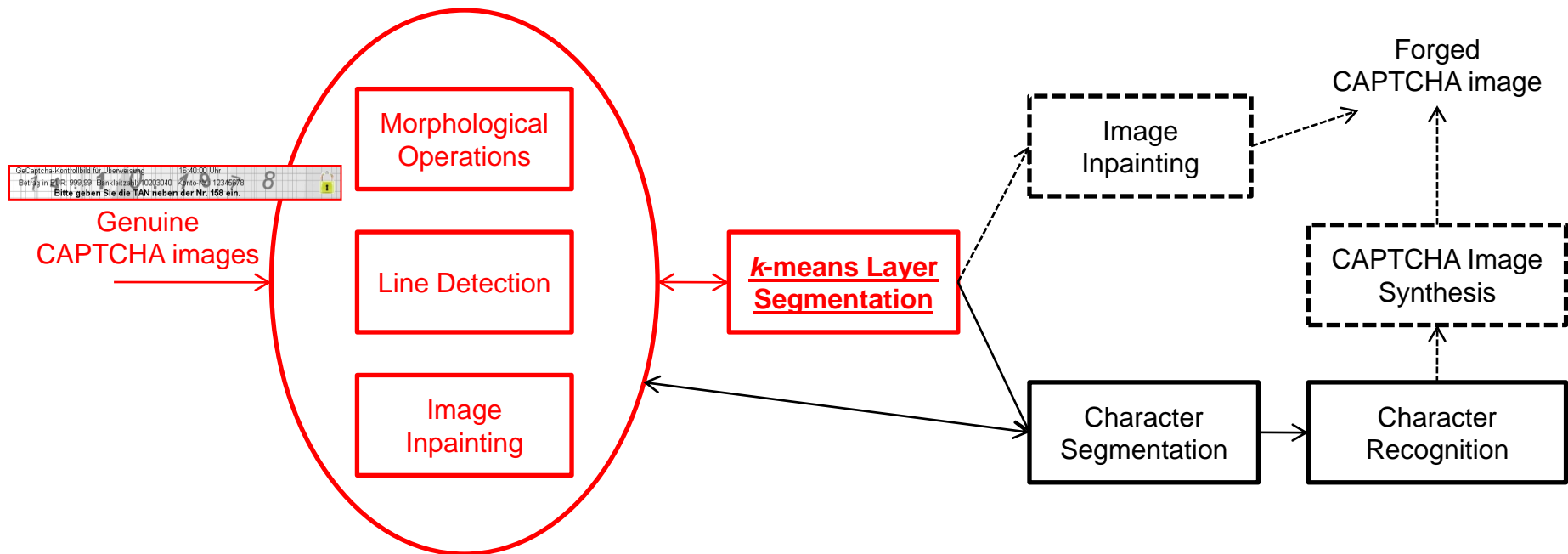
# How to forge a GeCaptcha image?

## Automated Attack 2 (Stage 1)



# How to forge a GeCaptcha image?

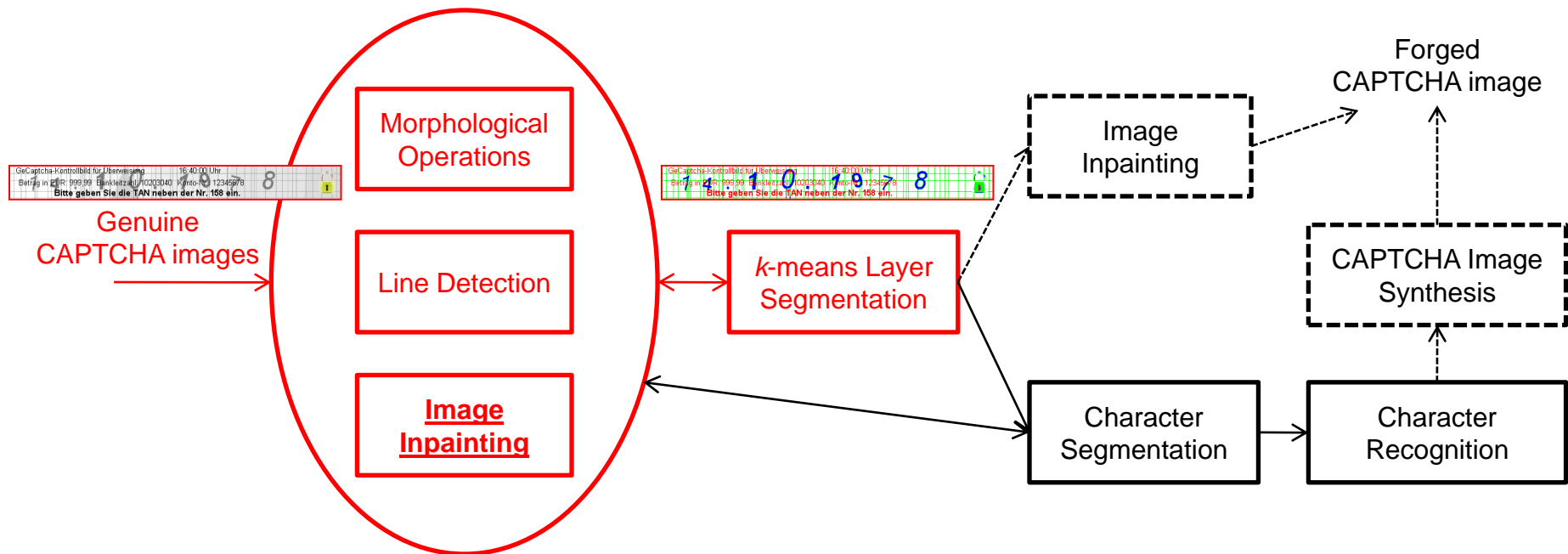
## Automated Attack 2 (Stage 1)





# How to forge a GeCaptcha image?

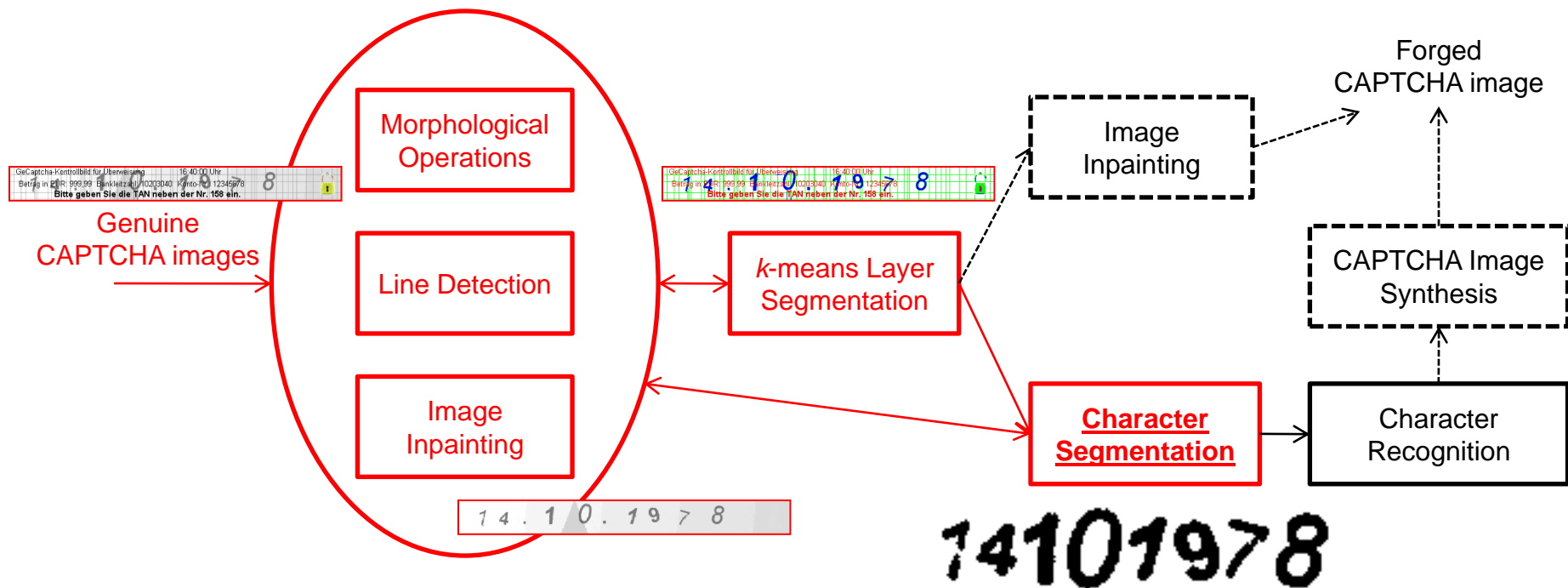
## Automated Attack 2 (Stage 1)





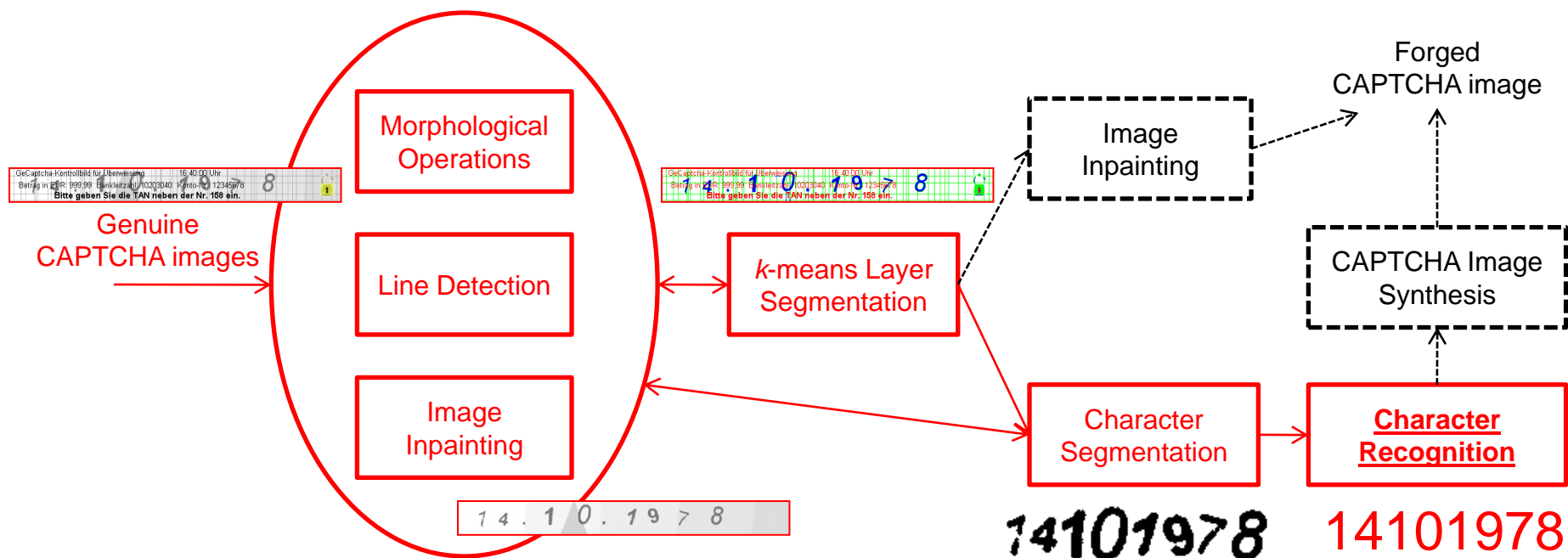
# How to forge a GeCaptcha image?

## Automated Attack 2 (Stage 1)



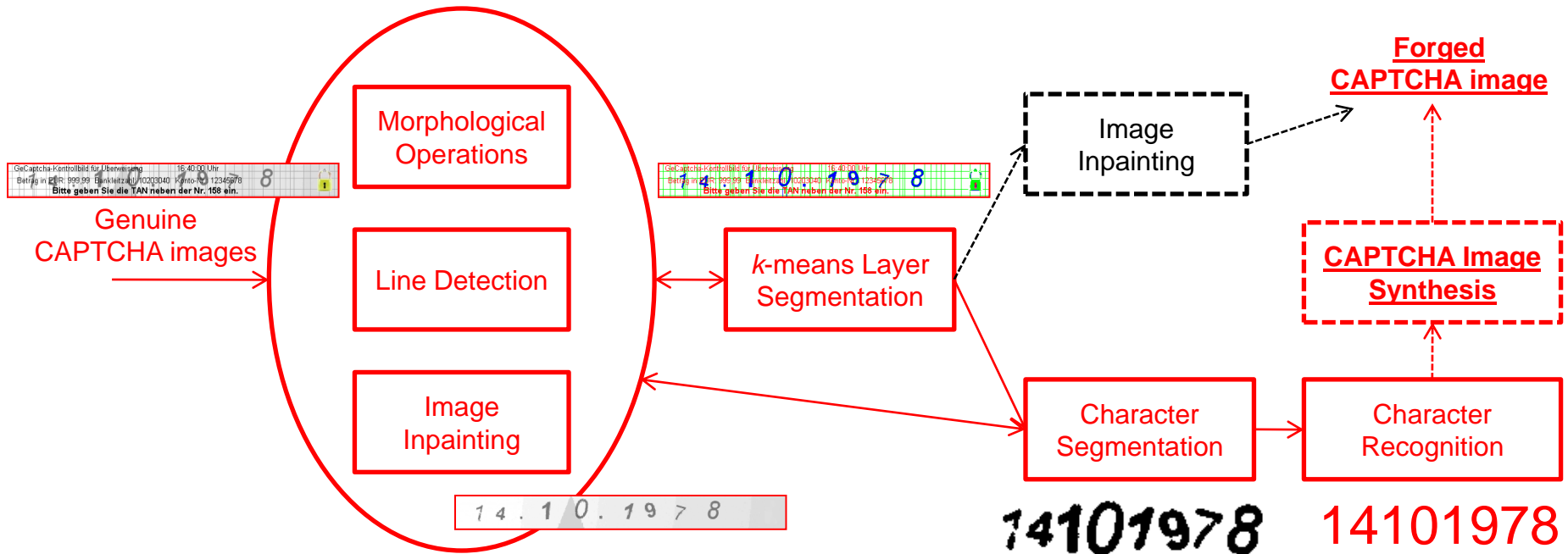
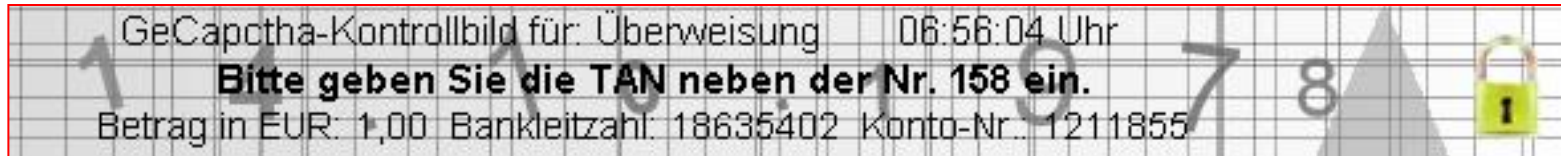
# How to forge a GeCaptcha image?

## Automated Attack 2 (Stage 1)



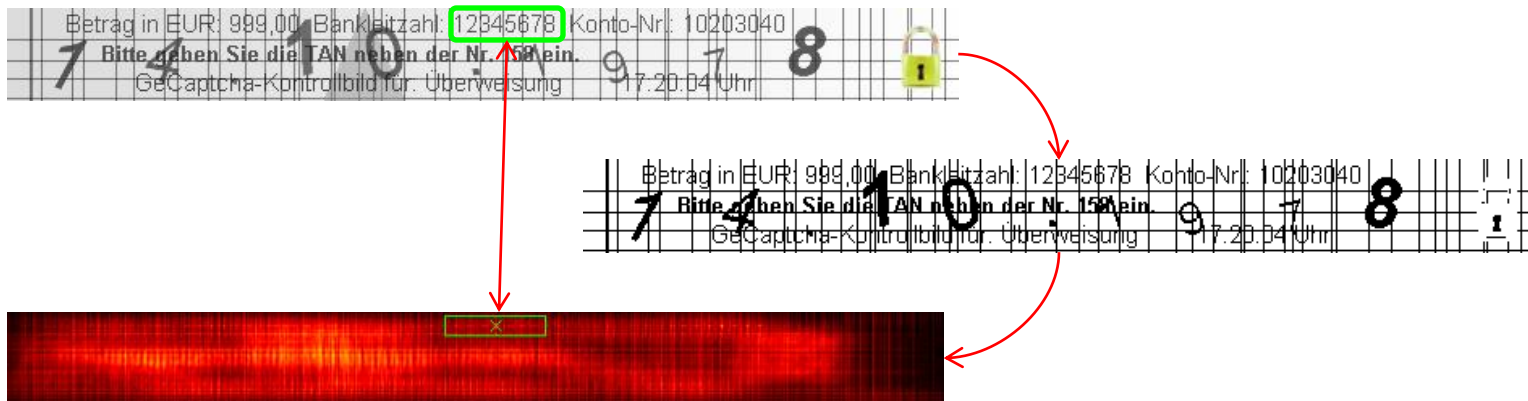
# How to forge a GeCaptcha image?

## Automated Attack 2 (Stage 2)



# Can GeCaptcha be enhanced?

- JPEG lossy compression does not help
  - Automated Attack 1 still works fine.
- Change all foreground layers/objects to have the same range of gray values
  - Both automated attacks fail.
  - More advanced attacks can be developed.



# Our communications with affected financial institutions

- German banks and e-banking service provider
  - The IT departments were reached and showed worry about publicity our research on their reputation.
- Chinese banks
  - We never reached the IT department of any bank.
  - In fact we have trouble finding the right person.
  - On the bank's web site, there is often NO any information about how to reach the IT department.
  - Calling the hotlines didn't help to get further information.
  - The bank hotlines seem to be polite but indifferent, but they are not the right people who should worry such things.

# Our communications with affected financial institutions

- American financial institutions
  - All the affected CAPTCHAs are technically supported by a single e-banking service provider.
  - We didn't get any response from this e-banking service provider.
- Financial institutions in other countries
  - We gave up due to the frustration we had for German, Chinese and American financial institutions.
- Observations and conclusion
  - So far, no affected banks have taken actions.
  - Who are representing banks technically and who is really caring about the consequences of e-banking insecurity?

# German authorities are still recommending GeCaptcha...

- Recently a joint fact-finding commission of two German states (Baden-Württemberg and Nordrhein-Westfalen) released a public press about the discovery of an organized crime of using e-banking Trojans to manipulate transactions.
  - 2.5 million PCs worldwide and 400,000 ones in Germany were infected.
  - 1.65 million Euro was involved.
  - Indexed TAN is the main target.
  - GeCaptcha is still one of the recommended “secure” e-banking solutions...