

Methodological issues in:

“Re: CAPTCHAS. Understanding CAPTCHA-solving services in an economic context”

Stefan Savage
University of California, San Diego

First, hypothetical measurement project

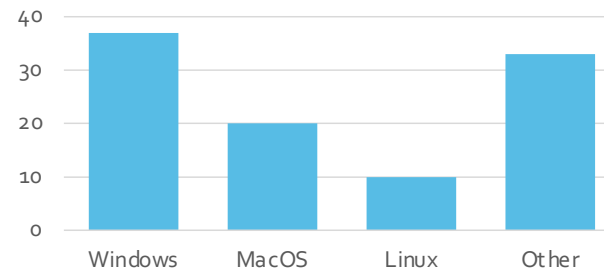
You have a hypothesis that organizational IT is becoming more homogeneous (i.e. companies are standardizing on windows, mac, linux, etc)

You notice that the nmap scanning tool has an “OS inference” mode

- It sends various kinds of UDP and TCP packets and uses the responses to infer what the host OS is

Your idea is to use nmap to scan the whole IPv4 Internet (4B addresses) and infer the OS type of each machine and then do it again in a year to see what has changed

Initial results (i.e., after scanning 4B IP addresses once)



What kinds of concerns might you have at this point?

Before you commit to this methodology, how might you try to validate this?

Do you need to look at all 4B addresses?

What is a CAPTCHA?

CAPTCHA: Using Hard AI Problems For Security

Luis von Ahn¹, Manuel Blum¹, Nicholas J. Hopper¹, and John Langford²

¹ Computer Science Dept., Carnegie Mellon University, Pittsburgh PA 15213, USA

² IBM T.J. Watson Research Center, Yorktown Heights NY 10598, USA

A CAPTCHA is a program that can generate and grade tests that: (A) most humans can pass, but (B) current computer programs can't pass. Such a program can be used to differentiate humans from computers and has many applications for practical security.

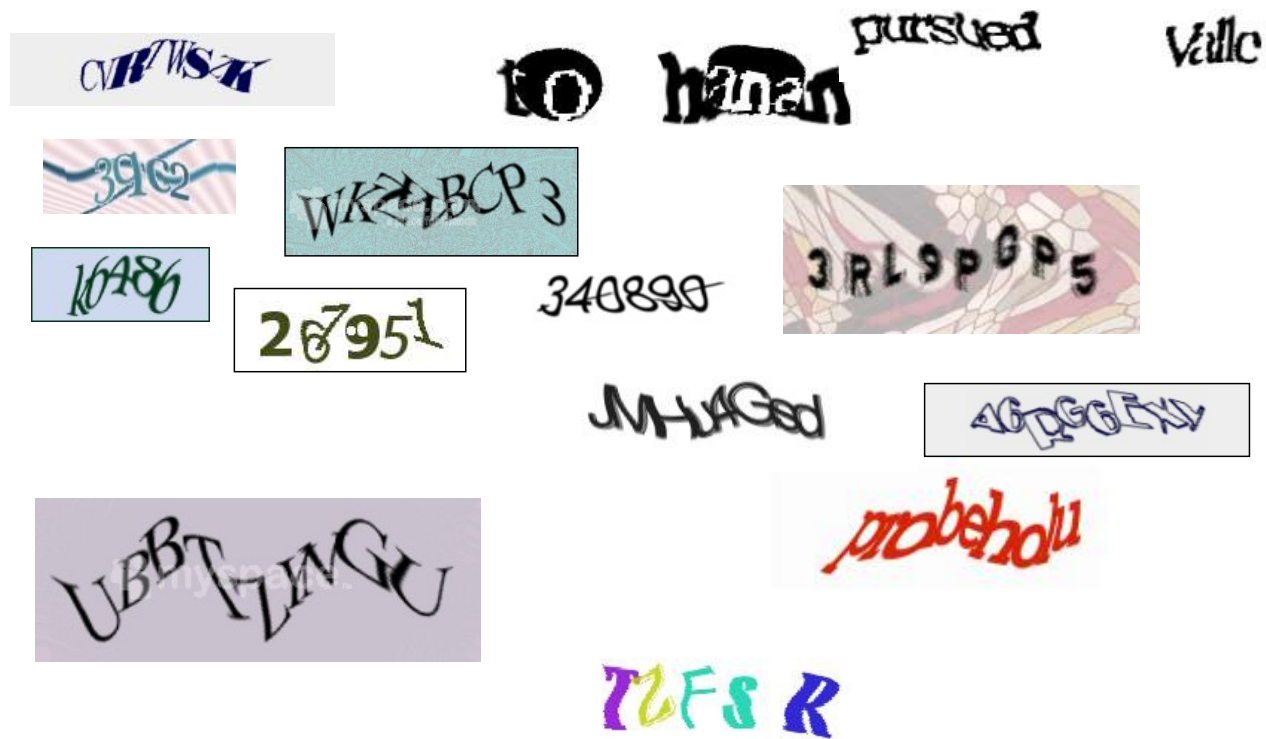
ication. CAPTCHAs based on these AI problem families, then, imply a win-win situation: either the problems remain unsolved and there is a way to differentiate humans from computers, or the problems are solved and there is a way to communicate covertly on some channels.

1 Introduction

A CAPTCHA is a program that can generate and grade tests that: (A) most humans can pass, but (B) current computer programs can't pass. Such a program can be used to differentiate humans from computers and has many applications for practical security, including (but not limited to):

- **Online Polls.** In November 1999, *slashdot.com* released an online poll asking which was the best graduate school in computer science (a dangerous question to ask over the web!). As is the case with most online polls, IP addresses of voters were recorded in order to prevent single users from voting more than once. However, students at Carnegie Mellon found a way to

CAPTCHAs circa 2008



What problem causes us to use CAPTCHAs?

Services with “free” accounts

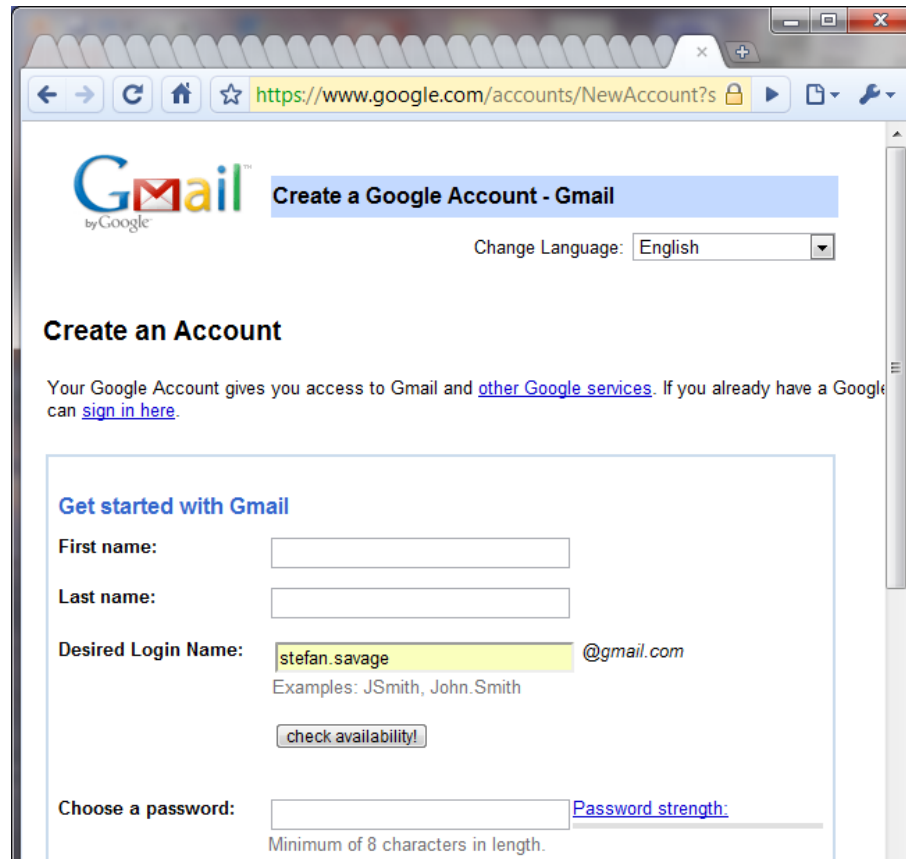
- E.g., e-mail, blogs, online social networks, etc
- How are these services monetized?

Key threat: free resources have value

- E-mail account -> spam/phishing
- Blog post -> Search Engine Optimization (SEO)
- OSN account -> click fraud

Bots can easily create millions of “fake” users (and do)

Account signup challenges (*main use at the time*)



A screenshot of a web browser window showing the Gmail account creation page. The browser's address bar displays the URL <https://www.google.com/accounts/NewAccount?s>. The page features the Gmail logo and a blue header bar with the text "Create a Google Account - Gmail". A language dropdown menu is set to "English". The main heading is "Create an Account", followed by a paragraph explaining the benefits of a Google Account and a link to sign in. The "Get started with Gmail" section contains input fields for "First name" and "Last name". The "Desired Login Name" field contains "stefan.savage" with "@gmail.com" appended, and examples "JSmith, John.Smith" are shown below. A "check availability!" button is present. The "Choose a password:" field is empty, with a "Password strength:" indicator and a note "Minimum of 8 characters in length."

<https://www.google.com/accounts/NewAccount?s>

Gmail
by Google

Create a Google Account - Gmail

Change Language: English

Create an Account

Your Google Account gives you access to Gmail and [other Google services](#). If you already have a Google Account, you can [sign in here](#).

Get started with Gmail

First name:

Last name:

Desired Login Name: @gmail.com
Examples: JSmith, John.Smith

Choose a password: [Password strength:](#)

Minimum of 8 characters in length.

Account signup challenges (*main use at the time*)

Security Question:	Choose a question ... If you forget your password we will ask for the answer to your security question. Learn More
Answer:	
Recovery email:	This address is used to authenticate your account should you ever encounter problems or forget your password. If you do not have another email address, you may leave this field blank. Learn More
Location:	United States
Birthday:	MM/DD/YYYY (e.g. "9/13/2010")
Word Verification:	Type the characters you see in the picture below.  & Letters are not case-sensitive

Are CAPTCHAs a good idea?

Ignore paper for now

What are the positives of using CAPTCHAs?

- How might we measure this as a provider?
- Easy or hard? What assumptions?

What are the negatives of using CAPTCHAs?

- How might we measure this as a provider?
- Easy or hard? What assumptions?

Paper idea

Measuring security is hard!

- What do we measure? What units? What assumptions about attackers?

Reframe via economics

- There is a third-party market for solving CAPTCHAs
 - Aside: why does this market exist?
- The *price* to solve a CAPTCHA is a proxy for how “hard” it is
 - What is the assumption here?
- Idea: The security offered by a CAPTCHA is the cost on the balance sheet of an attacker (i.e., the “tax” on their business model)
 - Note going retail rate (at the time) was ~\$1-2/1000 solves

Generalization: the price to defeat security is a proxy for the security offered

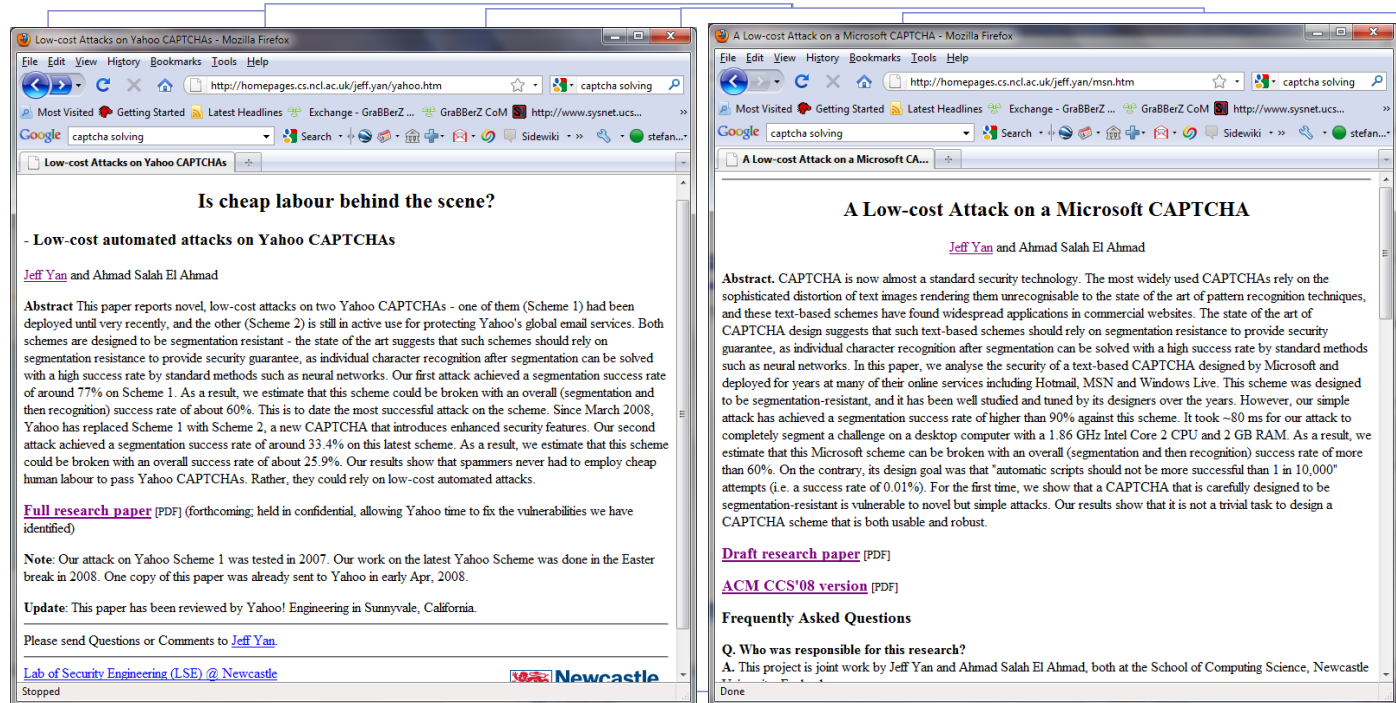
Software solving

Recall from von Ahn “**current** computer programs can’t pass”
(emphasis added)

- But surely, value will incent people to innovate and create such programs?

Yes! Researchers develop lots of solvers

When CAPTCHAs first became popular they were a challenge to the computer vision community





Slashdot | Windows Live Hotmail CAPTCHA Cracked, Exploited - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://tech.slashdot.org/article.pl?sid=08/04/15/1941236&from=rss

captcha solving

Most Visited Getting Started Latest Headlines Exchange - GraBBerZ ... GraBBerZ CoM http://www.sysnet.ucs... GraBBerZ CoM Cyber Genome Progra...

Google ez-grimpy Search Sidewiki Bookmarks Translate AutoLink AutoFill

Slashdot | Windows Live Hotmail ... mori_cvpr03.pdf (application/pdf O...

StefanSavage Preferences Subscribe Journal Submit Story Help Log Out

NEWS FOR NERDS. STUFF THAT MATTERS.

Search

Stories Recent Popular Search StefanSavage Why Subscribe?

▼ Slashdot

[Apple](#)

[Ask Slashdot](#)

[Book Reviews](#)

[Games](#)

[Hardware](#)

[Idle](#)

[Interviews](#)

[Linux](#)

[Mobile](#)

[Science](#)

[Technology](#)

[YRO](#)

▼ Site Info

[FAQ](#)

[Bugs](#)

[Code](#)

Windows Live Hotmail CAPTCHA Cracked, Exploited

Posted by kdawson on Tuesday April 15 2008, @03:28PM
from the nice-idea-while-it lasted dept.

[eldavojohn](#) passes along what may be the [last nail in the coffin](#) for CAPTCHA technology. Coming on the heels of credible accounts of the downfall of first [Yahoo's](#) and then [Gmail's](#) CAPTCHA, Ars Technica is reporting on Websense Security Labs' deconstruction of the [cracking](#) and [tuning / exploitation](#) of the Live Hotmail CAPTCHA. Ars calculates that a single zombie computer can sign up over 1400 Live Hotmail accounts in a day, and alternate account creation with spamming. Time to dust off [Kitten Auth](#)?

► internet security recaptcha haha slashdottedkitten story

Related Stories

► [IT: Yahoo CAPTCHA Hacked](#) 252 comments

► [IT: Gmail CAPTCHA Cracked](#) 317 comments

Submission: Hotmail Live Captcha Cracked by [eldavojohn](#) (898314)

► [Next-Generation CAPTCHA Exploits the Semantic Gap](#) 327 comments

► [Google's Audio CAPTCHA Falls To Automated Attack](#) 145 comments

► [IT: Fallout From the Fall of CAPTCHAs](#) 413 comments

► [Optical Character Recognition Still Struggling With Handwriting](#) 150 comments

TIME WARNER CABLE
THE POWER OF YOU™

GET A
\$100
REBATE

For New Customers Only



Digital Cable
with DVR &
no fees for HD

But... paper claims these weren't successful

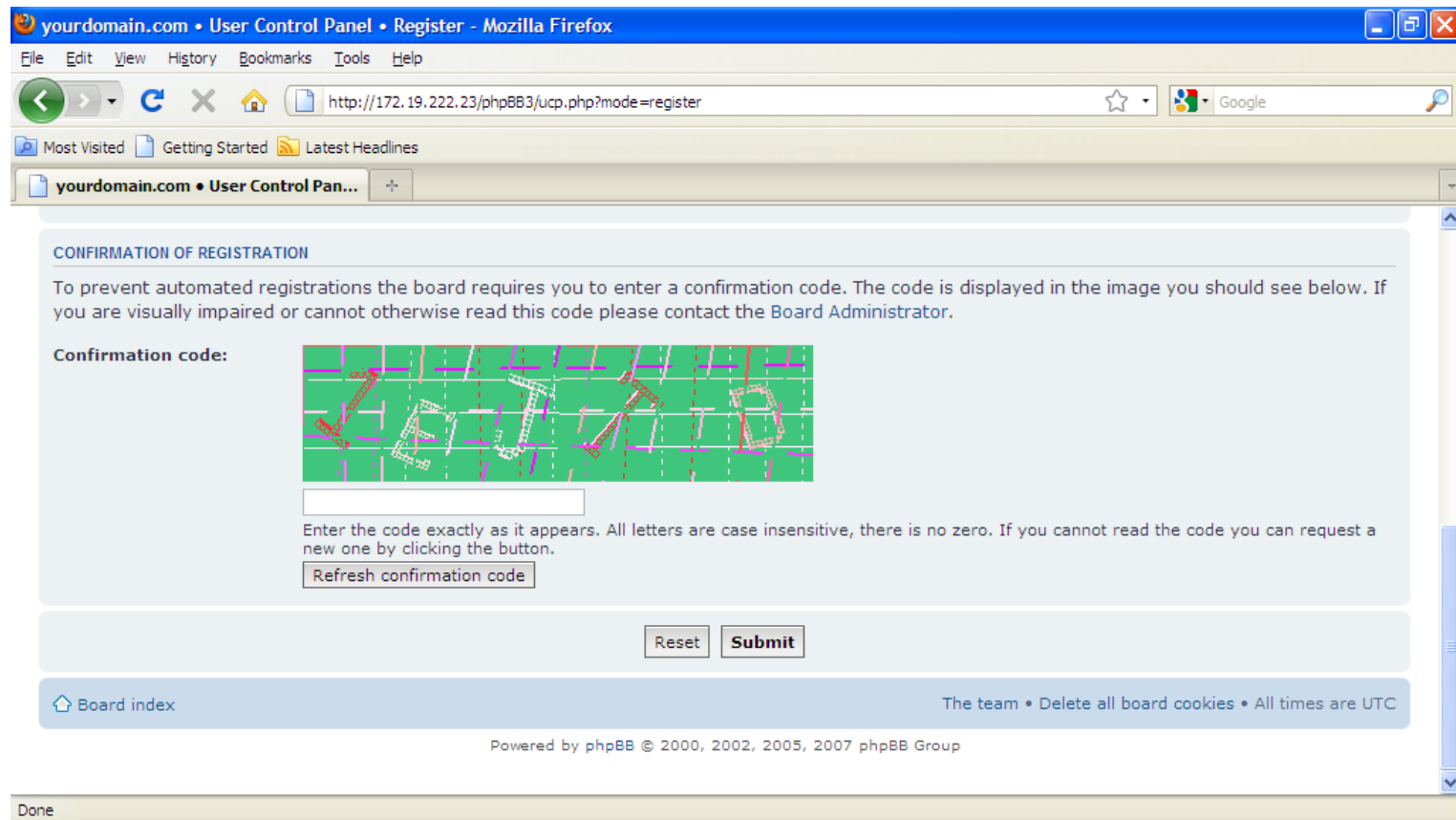
Argues that software solving is *technically feasible*,
but not *economically viable*

What evidence is provided for this claim?

XRumer:

Version 5.0.0 released in Oct 2008 with solvers for broad range of CAPTCHAs used in forums/blogs (mainly forum spammers)





XRumer 5.0.12, Copyright Botmaster.Net, Support ICQ 876975, Administration ICQ 111892

Project Tools Options Events log Scheduler Self-learning Plugins Update Help

XRumer 5.0 palladium

✉ 🏠 ?

Current project: Template ... On site XRumer 5.0.12 + Hrefer 2.99

Links database Reports Mail Anonymity Multithreading settings

Successful (43) Part Successful Profiles (36) Activation required The rest (57) 🚫

Posting control: active threads 0

Current position: 0 

Start Resume from the last position ▶ Stop

Posting 172.19.222.23/phpBB3 Test >>>

	Progress	Link	Status
1			
3		http://172.19.222.23/phpBB3/viewtopic.php?f=3&t=46	captcha decoded (4 attempts);registered (100%);profile edited;logged in;success - posted to "spam";

Authorization completed successfully.

Qualitative measurement

Obtain and test *time-matched* versions of XRumer and forum software

- How well did it work at various times?

Pattern emerges

- XRumer 5.0: solved CAPTCHAs in contemporaneous versions of Invision Power Board (IPB), phpBB, Simple Machine Forums (SMF), vBulletin
- Shortly thereafter new versions of those systems released with modified CAPTCHA not solved by 5.0

Arms race between XRumer and forum developers

August 2009, XRumer gives up

- With version 5.0.9 (Aug 2009) moves to support third-party (claimed) human solving services, stops developing new solvers
- anti-captcha.com (antigate) and captchabot.com

Assessment of ReCaptchaOCR

Custom solver for reCaptcha



Reported to the public on Dec 15th (Wilkins)

- Authors obtained copy: ~30% accuracy against old reCaptcha and ~18% against current (at the time) reCaptcha

Dec 16th automated solving rolled into popular Decaptcher.com service (at 25% normal price)

Dec 24th reCaptcha changed to new version (blobs) Solver no longer effective.

Mr. E (who now?)

Sometimes “asking” is a research technique...

Reported purchasing and developing solvers for his service, but gave up on this strategy...

“It is a big waste of time.” – Mr. E

Argument about why software solvers fail

Consider the traditional security arms race

- Thought experiment (hypothetical)
 - Software: 10k dev cost, 20% accuracy vs
 - Human labor: \$0.5/1000 wholesale
- Must attempt 100 million CAPTCHAs (solving 20 million) without being noticed and CAPTCHA changed...
 - ... just to break even w/humans

Notice what's going on here...

A mix of qualitative analysis, empirical measurement and a logical argument to try to explain findings

Why not a straight up quantitative analysis?

What might the counterfactuals be here?
(i.e., why might they be wrong)

Human solving

First starts to emerge in late 2006

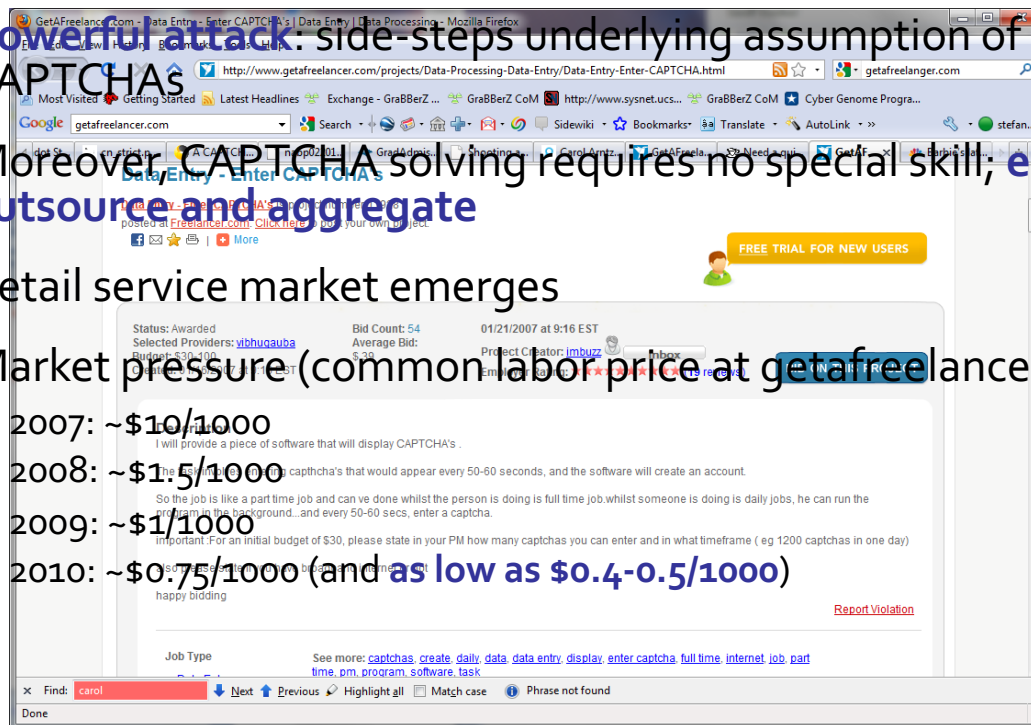
Powerful attack: side-steps underlying assumption of CAPTCHAs

Moreover, CAPTCHA solving requires no special skill; **easy to outsource and aggregate**

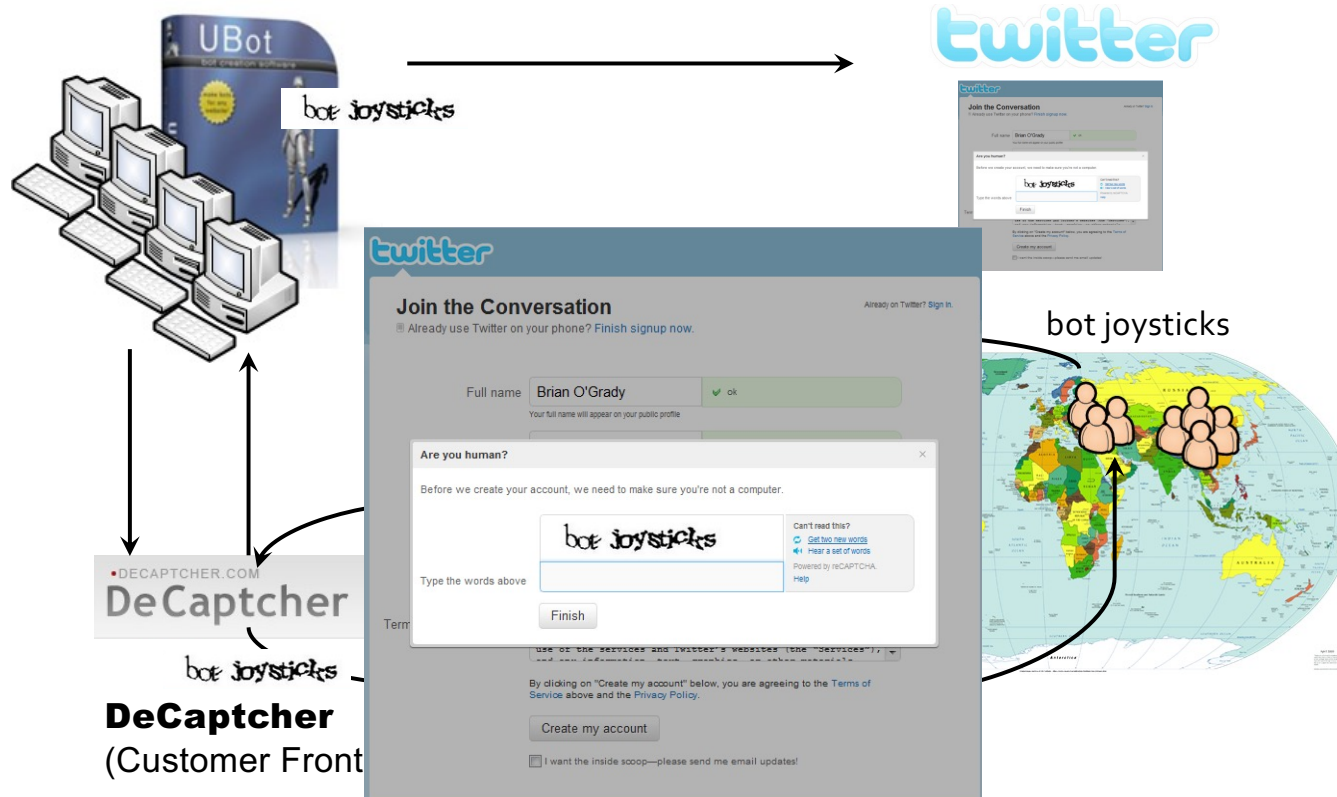
Retail service market emerges

Market pressure (common labor price at getafreelancer)

- 2007: ~\$10/1000
- 2008: ~\$1.5/1000
- 2009: ~\$1/1000
- 2010: ~\$0.75/1000 (and as low as \$0.4-0.5/1000)



Human solver services



Overall methodology

Signed up as service customers (8 services)

- Are these representative services?
- Pay for CAPTCHAs to be solved
(26 distinct commercial CAPTCHAs, plus custom-designed challenges)
Every 5 minutes for every service..
- Use to probe behavior of service under different conditions

Sign up as laborers (2 “job sites” matched with service)

- Kolotibablo → Antigate
- Pixprofit → Decaptcher
- Monitor which CAPTCHAs asked to solve

Let run for months...

Legal/Ethical issues

Ok to pay services that are abetting criminals?

Ok to solve CAPTCHAs?

Is this human subjects research?

Why even look at the worker side?

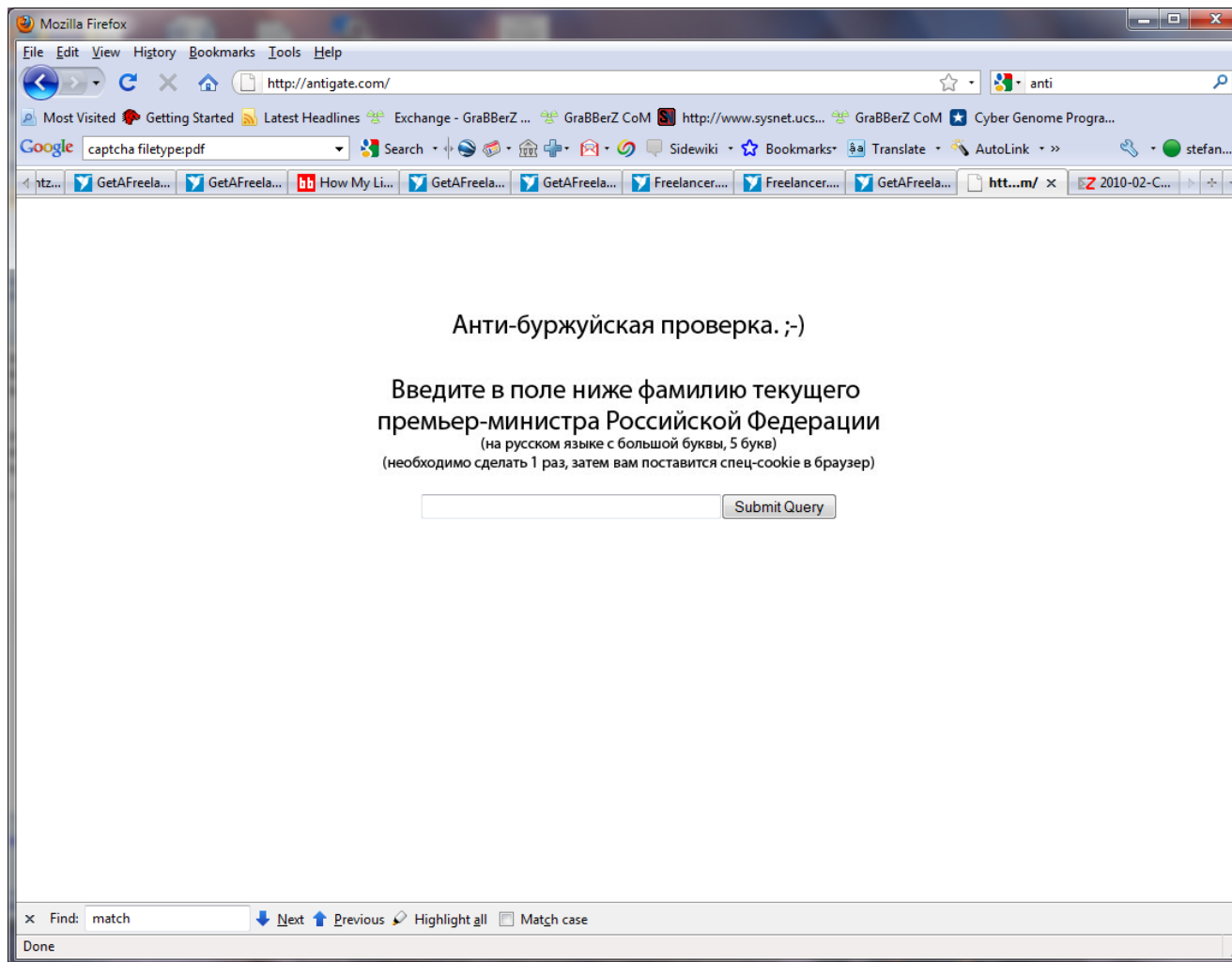
What can be learned?

- Validate that solving works as hypothesized (sometimes you get surprised)
E.g., how do they incentivize high quality work?
- Validate labor “cut” of retail price
- Measure CAPTCHA makeup



PixPro
CAP
HA





Aside: qualitative evidence of demand pressure

Message to workers at typethat.biz:

009-12-14 13:54 Admin post

Hello, as you could see, server was unstable last days. We can't get more captchas because of too high prices in comparison with other services. To solve this problem, unfortunately we have to change the rate, on Tuesday it will be reduced.

Price reduced from \$1/1000 to \$0.75/1000 shortly thereafter

Three kinds of results on customer side

How well do the human solver services do?

- Raw results
- Economic interpretation of results

How much load can they handle?

Geographic information about workers?

Accuracy

Service	Dates (2009–2010)	Requests	Correct	Incorrect	Rejected
Antigate	Oct 06 – Feb 01 (118 days)	28210	22933 (82.7%)	4793 (17.3%)	484 (1.7%)
BeatCaptchas	Sep 21 – Feb 01 (133 days)	28303	22282 (86.7%)	3430 (13.3%)	2591 (9.2%)
BypassCaptcha	Sep 23 – Feb 01 (131 days)	28117	21167 (76.3%)	6562 (23.7%)	388 (1.4%)
CaptchaBot	Oct 06 – Feb 01 (118 days)	28187	18628 (82.1%)	4049 (17.9%)	5510 (19.5%)
CaptchaBypass	Sep 23 – Dec 23 (91 days)	17739	13018 (82.0%)	2851 (18%)	1870 (10.5%)
CaptchaGateway	Oct 21 – Nov 03 (13 days)	1803	1475 (86.0%)	240 (14.0%)	88 (4.9%)
Decaptcher	Sep 21 – Feb 01 (133 days)	28284	21009 (86.1%)	3402 (13.9%)	3873 (14%)
ImageToText	Oct 06 – Feb 01 (118 days)	14321	11353 (85.7%)	1893 (14.3%)	1075 (7.5%)

Methodology

- Solved CAPTCHA every 5 mins per service
- Rotated between 25 types

Findings

- 80%+ accuracy on 7 of 8 services (when answers given)
- Availability varies **considerably** (98.6% vs 80.5%)
- Implications? Why do we care?

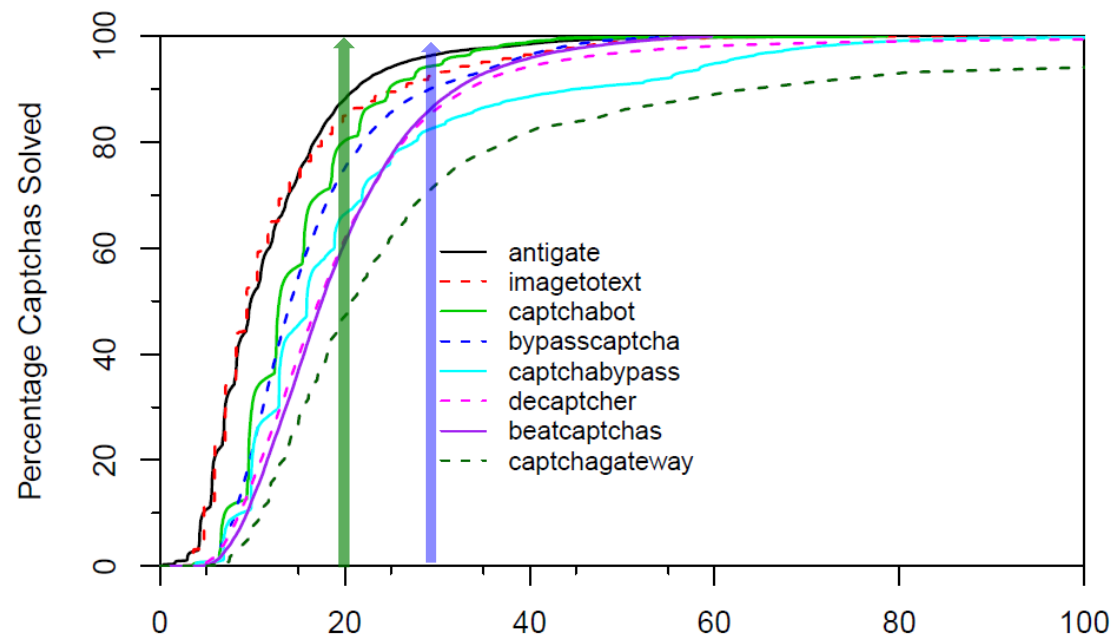
But... how do we know if a solution is accurate?!?

What were the options/tradeoffs here?

What does paper do?

- Get many solutions for each CAPTCHA; pick plurality
- How to validate that approach?
 - Validate via random sampling of 1025 CAPTCHAs; label by hand and finds 7% error rate in plurality algorithm
 - What about sampling error?

Response time

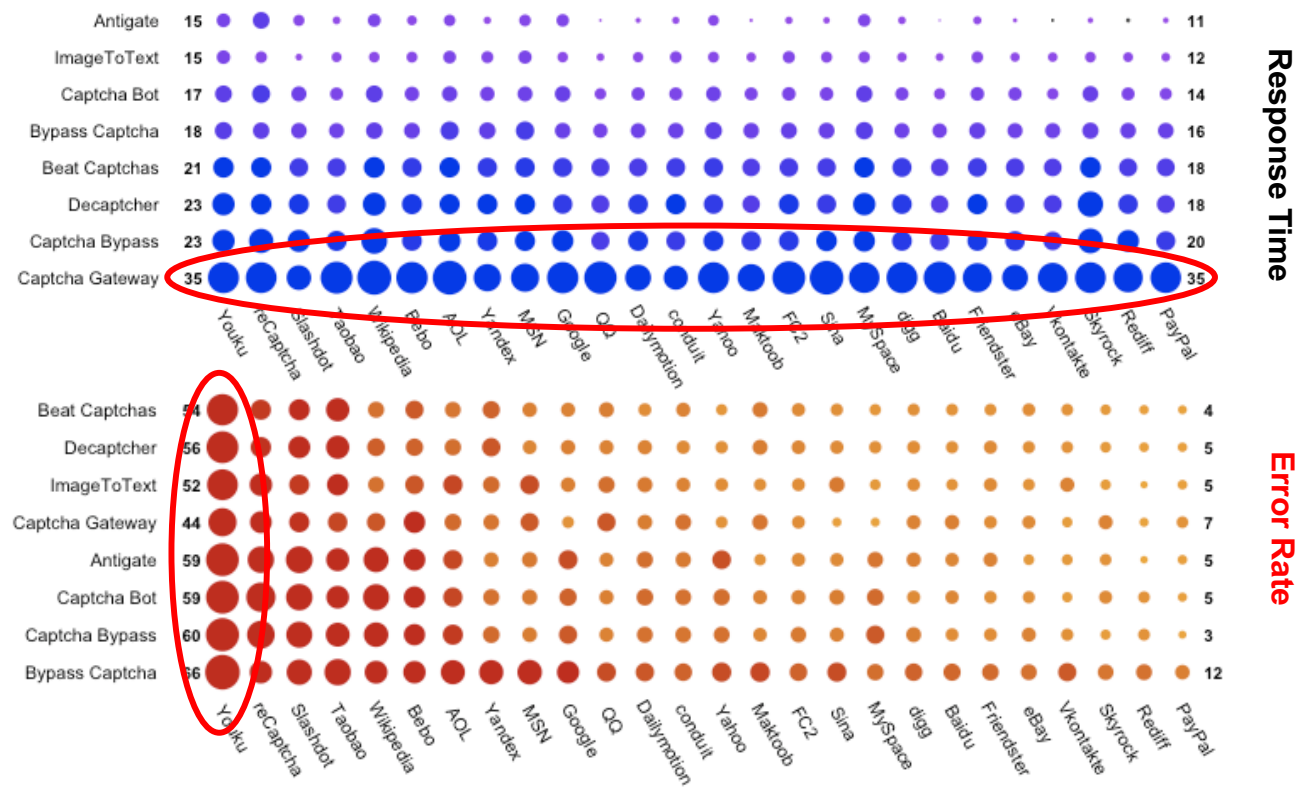


Median response time ~20 seconds or better

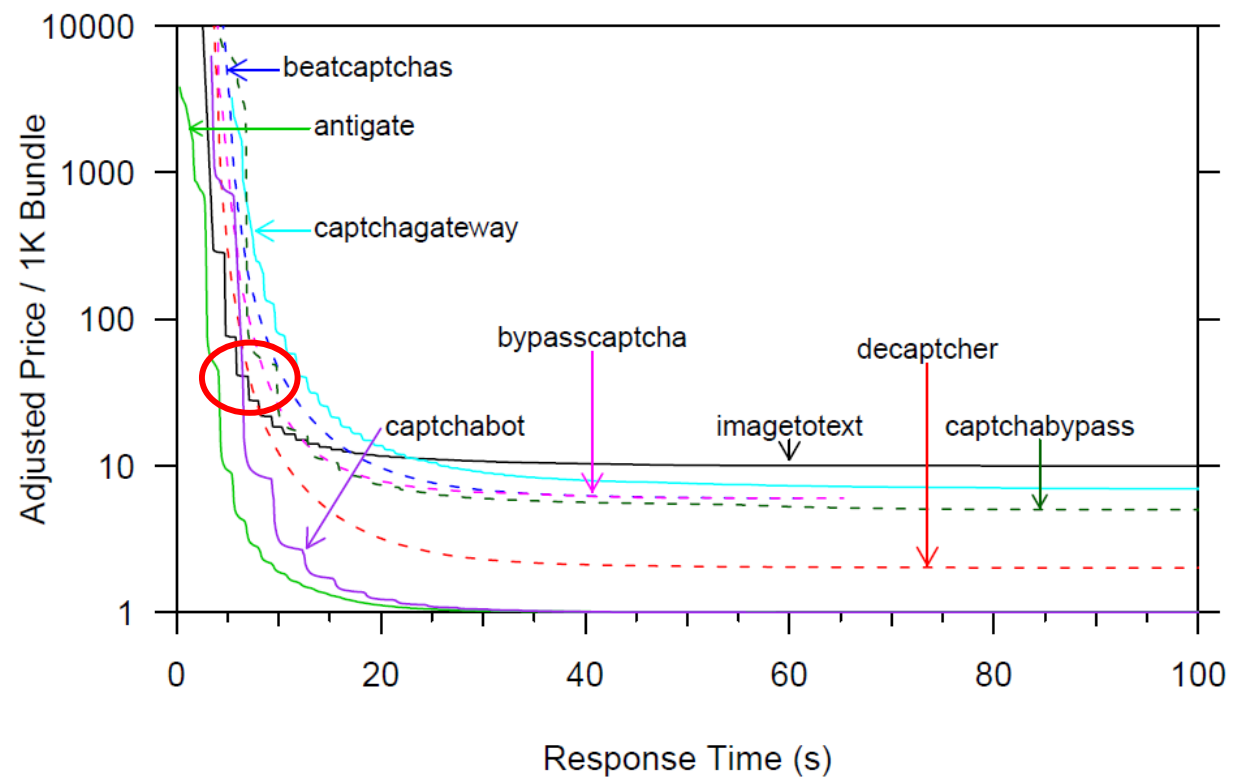
80% or more within ~30 seconds

Why do we care about this?

Impact of CAPTCHA type on response time & accuracy (do we care?)



Value (\$/CAPTCHA in time)



Capacity (how many workers)

- Methodology: Incrementally increased load
 - 32-1536 threads submitting Yahoo CAPTCHAs until response rate maxes out
- Results in solutions/sec:

“We have fixed workers which will support the basic volume. We will call for more workers when [a] bigger volume come[s].” -Mr. E (service operator)

Labor demographics

Which labor markets are driving CAPTCHA-solving?

Idea: get CAPTCHA solvers to reveal information about their country or location

Two approaches

- Language CAPTCHA: asks for word to digit translation in 20+ languages
- Local time CAPTCHA: asks for current time in 14 languages

Введите показанные цифры

ч 请输入当前时间 ть

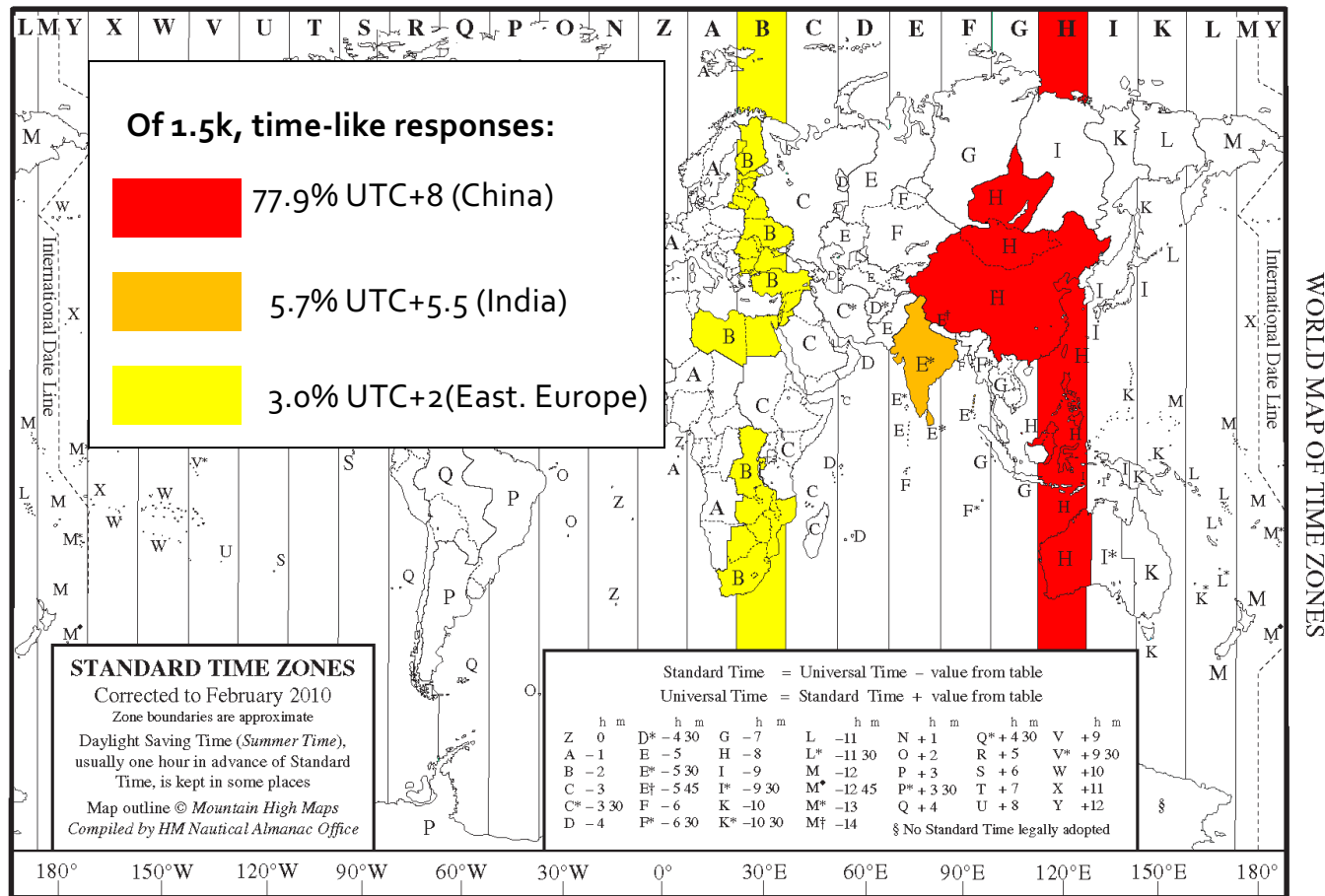
--	--	--	--

Language	Example	AG	BC	BY	CB	DC	IT	All
English	one two three	51.1	37.6	4.76	40.6	39.0	62.0	39.2
Chinese (Simp.)	一 二 三	48.4	31.0	0.00	68.9	26.9	35.8	35.2
Chinese (Trad.)	一 二 三	52.9	24.4	0.00	63.8	30.2	33.0	34.1
Spanish	uno dos tres	1.81	13.8	0.00	2.90	7.78	56.8	13.9
Italian	uno due tre	3.65	8.45	0.00	4.65	5.44	57.1	13.2
Tagalog	isá dalawá tatlo	0.00	5.79	0.00	0.00	7.84	57.2	11.8
Portuguese	um dois três	3.15	10.1	0.00	1.48	3.98	48.9	11.3
Russian	один два три	24.1	0.00	0.00	11.4	0.55	16.5	8.76
Tamil	ஒன்று இரண்டு மூன்று	2.26	21.1	3.26	0.74	12.1	5.36	7.47
Dutch	een twee drie	4.09	1.36	0.00	0.00	1.22	31.1	6.30
Hindi	एक दो तीन	10.5	5.38	2.47	1.52	6.30	9.49	5.94

Lower cost connected labor markets (China, India, Russia)
well represented (esp China)

Greek	ένα δύο τρία	0.45	0.00	0.00	0.00	0.00	15.5	2.65
Arabic	واحد اثنين ثلاثة	0.00	0.00	0.00	0.00	0.00	15.3	2.56

- Data: submitted 222 unique CAPTCHAs per language
- Table: shows percent correct for language per service



Discussion issues

Tries to use data to advance economic view on

- CAPTCHAs are not a technical defense in the classic sense, but an **economic filter**
- Filters out attackers without effective business models
 - Expected value of resource >> value of CAPTCHA
 - Spam: ~300 messages/account to break even at those prices (if one believed spamalytics paper)

Lots of other efforts then use this model

- Impact of MFA on underground price of bulk gmail accounts
- Impact of mass takedown on underground price of bulk twitter accounts

Questions?

For next time

Deepak Kumar, Patrick Gage Kelley, Sunny Consolvo, Joshua Mason, Elie Bursztein, Zakir Durumeric, Kurt Thomas, Michael Bailey. [Designing Toxic Content Classification for a Diversity of Perspectives](#), In *Proceedings of the USENIX Symposium on Usable Privacy and Security*, August, 2021.

Guest lecture by Deepak Kumar – in person