ECE 498KL: eCrime and Internet Service Abuse
CAPTCHAs
Kirill Levchenko
December 4, 2018
Major Commodities

❖ Web traffic (categorized by topic and country origin)
  • Topics: gambling, pharma, adult, etc.
  • Origin: US, EU, Asia, Mix, etc.
  • Sources: SEO, spam, ads, bots, resale, etc.
  • Monetization: affiliate marketing, click fraud, resale

❖ Installs (categorized by target country)
  • Target: US, EU, Asia, Mix, etc.
  • Sources: compromise (Web, email, etc.), trojans, resale, etc.
  • Monetization: bots (e.g. spam), ransomware, fake AV, etc.
Abusers may subtly use social networking sites for marketing purposes. The accounts on social networking sites can also be used for SEO purposes. For example, abusers may create retailer's product consistently appear near the top of the search results. Abusers can use social networking sites to build backlinks consistently to increase the ranking of websites. Some of the search results will be generated for the search terms related to the query. The search terms are generated by the abusers who use SEO as a means of producing high-quality SEO content. The SEO articles can be created through various methods, including article rewriting, plagiarism detection, and CAPTCHA solvers. The abusers can then implement various monetization schemes with the accounts, most of them involving the monetization of the search results. Abusers can create a retailer's product consistently appear near the top of the search results. The most direct form of spamming utilizes the search results. The abusers can use social networking sites to build backlinks consistently to increase the ranking of websites. The search terms are generated by the abusers who use SEO as a means of producing high-quality SEO content. The SEO articles can be created through various methods, including article rewriting, plagiarism detection, and CAPTCHA solvers. The abusers can then implement various monetization schemes with the accounts, most of them involving the monetization of the search results. Abusers can create a retailer's product consistently appear near the top of the search results. The most direct form of spamming utilizes the search results.
CAPTCHAs

pursued

Valle

Select all squares that match the label: Sarah Connor.
If there are none, click skip.

Milwaukee - them -

redcoats president
CAPTCHA: Using Hard AI Problems for Security

Luis von Ahn\textsuperscript{1}, Manuel Blum\textsuperscript{1}, Nicholas J. Hopper\textsuperscript{1}, and John Langford\textsuperscript{2}

\textsuperscript{1} Computer Science Dept., Carnegie Mellon University, Pittsburgh PA 15213, USA
\textsuperscript{2} IBM T.J. Watson Research Center, Yorktown Heights NY 10598, USA

Abstract. We introduce \texttt{CAPTCHA}, an automated test that humans can pass, but current computer programs can’t pass: any program that has high success over a \texttt{CAPTCHA} can be used to solve an unsolved Artificial Intelligence (AI) problem. We provide several novel constructions of \texttt{CAPTCHAs}. Since \texttt{CAPTCHAs} have many applications in practical security, our approach introduces a new class of hard problems that can be exploited for security purposes. Much like research in cryptography has had a positive impact on algorithms for factoring and discrete log, we hope that the use of hard AI problems for security purposes allows us to advance the field of Artificial Intelligence. We introduce two families of AI problems that can be used to construct \texttt{CAPTCHAs} and we show that solutions to such problems can be used for steganographic communication. \texttt{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 stuff the ballots by using programs that voted for CMU thousands of times. CMU’s score started growing rapidly. The next day, students at MIT wrote their own voting program and the poll became a contest between voting “bots”. MIT finished with 21,156 votes, Carnegie Mellon with 21,032 and every other school with less than 1,000. Can the result of any online poll be trusted? Not unless the poll requires that only humans can vote.
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):
Cheapest price on the market
Starting from 0.5USD per 1000 images, depending on your daily upload volume
Engaged with 8 major CAPTCHA-solving services

Submitted 7,500 instances of 25 different CAPTCHAs
- Microsoft, Google, Yahoo, PayPal, eBay, QQ, Baidu, Yandex, etc.

Measured accuracy, response time, throughput, adaptability

**Median Error Rate**
- BeatCaptcha: 10.3%
- Decaptcha: 10.3%
- ImageToText: 11.3%
- CaptchaGateway: 11.9%
- Antigate: 12.4%
- CaptchaBot: 13.3%
- CaptchaBypass: 13.4%
- BypassCaptcha: 19.9%

**Median Response Time (seconds)**
- BeatCaptcha: 17.3
- Decaptcha: 17.1
- ImageToText: 17.4
- CaptchaGateway: 21.3
- Antigate: 9.6
- CaptchaBot: 12.8
- CaptchaBypass: 15.9
- BypassCaptcha: 14.1

Automated CAPTCHA Solving

- Can CAPTCHAs be solved automatically?
- Hard to automatically solve all possible CAPTCHAs
- May be possible to build solver for specific family
Automated CAPTCHA Solving

- Xrumer 5.0.0 released in Oct 2008 with solvers for broad range of CAPTCHAs used in forums/blogs
Automated CAPTCHA Solving

- Reported to the public on Dec 15, 2009
  - Approx. 30% accuracy against old reCaptcha and 18% against current (at the time) reCaptcha
- Dec 16, 2009 automated solving rolled into popular Decaptcher.com service (at 25% normal price)
- Dec 24, 2009 reCaptcha changed to modern version (blobs): Solver no longer effective.
Automated CAPTCHA Solving

- **Solvers are fragile:**
  Easy to change CAPTCHA to break current generation of solvers that are tuned for specific family

- Cost of developing automated solver is high
  - Requires highly skilled labor and time

- How many does an automated solver have to solve to break even?
CAPTCHA solving service

- Cheapest price on the market
  Starting from 0.5USD per 1000 images, depending on your daily upload volume

- Pay as you go
  Pay-per-captcha payment basis. Minimum refill is 1 USD, no recurring charges

- 99.99% uptime since 2007
  Vast amount of workers and premium infrastructure allows us to provide highly reliable 24/7/365 service

registration

Client area

1

Your app uploads a captcha to our server
1. Your app uploads a captcha to our server

- Easy API integration
- Unlimited number of simultaneous uploads
- High-speed request processing

2. We assign a worker for your captcha

100% of captchas are solved by human workers from around the world. This is why by using our service you help thousands of people to feed themselves and their families. Check out some of their stories here.
We assign a worker for your captcha

100% of captchas are solved by human workers from around the world. This is why by using our service you help thousands of people to feed themselves and their families. Check out some of their stories here.

An average worker makes about $100 per month which is a very good salary in such countries like India, Pakistan, Vietnam and others. With your help they now have a choice between working in polluted industries and working in front of a computer.
100% of captchas are solved by human workers from around the world. This is why by using our service you help them.

Priority: 0
Balance: 0.009

Send
Countdown: 27
10.0% of the funds are invested in the United Kingdom.

An additional 10.0% are invested in Venezuela.

The United States accounts for 15.0% of the investments.

N/A represents 20.0% of the investments.

Other countries make up the remaining 45.0%.
3 Worker types answer and we send it to your app

Average solving time  7.1 sec
Workers banned       1023255
TOTAL                514
24 H                 1%
ERRORS

Our advanced quality control system monitors worker's entries and quickly eliminates cheaters.
And by the way, we’re good as hell in solving Javascript captchas!

- Costs for Recaptcha: from 1.8 USD per 1000 solutions.
- Costs for Funcaptcha: from 1.8 USD per 1000 solutions.
- You don’t need to emulate browser and run javascripts.
- You send us “sitekey” or “public key” value.
- We give you “g-recaptcha-response” and you simply submit form with it.
CAPTCHA Study

• **Sign up as service customers** (8 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
    (our own CAPTCHAs “tagged” to allow easy identification)

• Let run for months…
Accuracy and Latency

<table>
<thead>
<tr>
<th>Service</th>
<th>Median Error Rate</th>
<th>Median Response Time (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BeatCaptchas</td>
<td>10.3%</td>
<td>17.3</td>
</tr>
<tr>
<td>Decaptcha</td>
<td>10.3%</td>
<td>17.1</td>
</tr>
<tr>
<td>ImageToText</td>
<td>11.3%</td>
<td>9.4</td>
</tr>
<tr>
<td>CaptchaGateway</td>
<td>11.9%</td>
<td>21.3</td>
</tr>
<tr>
<td>Antigate</td>
<td>12.4%</td>
<td>9.6</td>
</tr>
<tr>
<td>CaptchaBot</td>
<td>13.3%</td>
<td>12.8</td>
</tr>
<tr>
<td>CaptchaBypass</td>
<td>13.4%</td>
<td>15.9</td>
</tr>
<tr>
<td>BypassCaptcha</td>
<td>19.9%</td>
<td>14.1</td>
</tr>
</tbody>
</table>
CAPTCHA Types

![CAPTCHA Types Chart]

- **Antigate**: 15
- **ImageToText**: 15
- **Captcha Bot**: 17
- **Bypass Captcha**: 18
- **Beat Captchas**: 21
- **Decaptcher**: 23
- **Captcha Bypass**: 23
- **Captcha Gateway**: 35

**Response Time**
- **Beat Captchas**: 54
- **Decaptcher**: 56
- **ImageToText**: 52
- **Captcha Gateway**: 44
- **Antigate**: 59
- **Captcha Bot**: 59
- **Captcha Bypass**: 60
- **Bypass Captcha**: 66

**Error Rate**
Capacity

• Incrementally increased load (32-1536 threads)
  ✷ Each thread submitted new CAPTCHA after old one solved

• Unable to max Antigate out (41 CAPTCHAs/sec)

• Other services
  ✷ Decaptcha, Captchabot: max at 14-15/sec
  ✷ BeatCaptchas: max at 8/sec
  ✷ BypassCaptchas: max at 4/sec

• If we assume 10-13sec/CAPTCHA (and no other users)
  ✷ Antigate has at least 400-500 workers
  ✷ Decaptcha/Captchabot: 140-200 workers
  ✷ BeatCaptchas: 80-100 workers
  ✷ BypassCaptchas: 40-50 workers
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
<table>
<thead>
<tr>
<th>Language</th>
<th>Example</th>
<th>AG</th>
<th>BC</th>
<th>BY</th>
<th>CB</th>
<th>DC</th>
<th>IT</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>one two three</td>
<td>51.1</td>
<td>37.6</td>
<td>4.76</td>
<td>40.6</td>
<td>39.0</td>
<td>62.0</td>
<td>39.2</td>
</tr>
<tr>
<td>Chinese (Simp.)</td>
<td>— — —</td>
<td>48.4</td>
<td>31.0</td>
<td>0.00</td>
<td>68.9</td>
<td>26.9</td>
<td>35.8</td>
<td>35.2</td>
</tr>
<tr>
<td>Chinese (Trad.)</td>
<td>— — —</td>
<td>52.9</td>
<td>24.4</td>
<td>0.00</td>
<td>63.8</td>
<td>30.2</td>
<td>33.0</td>
<td>34.1</td>
</tr>
<tr>
<td>Spanish</td>
<td>uno dos tres</td>
<td>1.81</td>
<td>13.8</td>
<td>0.00</td>
<td>2.90</td>
<td>7.78</td>
<td>56.8</td>
<td>13.9</td>
</tr>
<tr>
<td>Italian</td>
<td>uno due tre</td>
<td>3.65</td>
<td>8.45</td>
<td>0.00</td>
<td>4.65</td>
<td>5.44</td>
<td>57.1</td>
<td>13.2</td>
</tr>
<tr>
<td>Tagalog</td>
<td>isá dalawá tatlí</td>
<td>0.00</td>
<td>5.79</td>
<td>0.00</td>
<td>0.00</td>
<td>7.84</td>
<td>57.2</td>
<td>11.8</td>
</tr>
<tr>
<td>Portuguese</td>
<td>um dois três</td>
<td>3.15</td>
<td>10.1</td>
<td>0.00</td>
<td>1.48</td>
<td>3.98</td>
<td>48.9</td>
<td>11.3</td>
</tr>
<tr>
<td>Russian</td>
<td>один два три</td>
<td>24.1</td>
<td>0.00</td>
<td>0.00</td>
<td>11.4</td>
<td>0.55</td>
<td>16.5</td>
<td>8.76</td>
</tr>
<tr>
<td>Tamil</td>
<td>ஒன்று இரண்டு</td>
<td>2.26</td>
<td>21.1</td>
<td>3.26</td>
<td>0.74</td>
<td>12.1</td>
<td>5.36</td>
<td>7.47</td>
</tr>
<tr>
<td>Dutch</td>
<td>een twee drie</td>
<td>4.09</td>
<td>1.36</td>
<td>0.00</td>
<td>0.00</td>
<td>1.22</td>
<td>31.1</td>
<td>6.30</td>
</tr>
<tr>
<td>Hindi</td>
<td>एक दो तीन</td>
<td>10.5</td>
<td>5.38</td>
<td>2.47</td>
<td>1.52</td>
<td>6.30</td>
<td>9.49</td>
<td>5.94</td>
</tr>
<tr>
<td>German</td>
<td>eins zwei drei</td>
<td>3.62</td>
<td>0.72</td>
<td>0.00</td>
<td>1.46</td>
<td>0.58</td>
<td>29.1</td>
<td>5.91</td>
</tr>
<tr>
<td>Malay</td>
<td>satu dua tiga</td>
<td>0.00</td>
<td>1.42</td>
<td>0.00</td>
<td>0.00</td>
<td>0.55</td>
<td>29.4</td>
<td>5.23</td>
</tr>
<tr>
<td>Vietnamese</td>
<td>một hai ba</td>
<td>0.46</td>
<td>2.07</td>
<td>0.00</td>
<td>0.00</td>
<td>1.74</td>
<td>18.1</td>
<td>3.72</td>
</tr>
<tr>
<td>Korean</td>
<td>일 이 삼</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>20.2</td>
<td>3.37</td>
</tr>
<tr>
<td>Greek</td>
<td>ἐνα δύο τρία</td>
<td>0.45</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>15.5</td>
<td>2.65</td>
</tr>
<tr>
<td>Arabic</td>
<td>ثلاثة اثنين واحد</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>15.3</td>
<td>2.56</td>
</tr>
<tr>
<td>Bengali</td>
<td>এক দুই তিন</td>
<td>0.45</td>
<td>0.00</td>
<td>9.89</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>1.72</td>
</tr>
<tr>
<td>Kannada</td>
<td>ಎರಡು ಚತುರ್ತರ</td>
<td>0.91</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.55</td>
<td>6.14</td>
<td>1.26</td>
</tr>
<tr>
<td>Klingon</td>
<td>ɾ &lt; &lt;</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>1.12</td>
<td>0.19</td>
</tr>
<tr>
<td>Farsi</td>
<td>سه دو یک</td>
<td>0.45</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.08</td>
</tr>
</tbody>
</table>
Time Zone

China
Adaptability

Find all cats • 请找所有猫 • Найдите кошек • बिल्लियाँ ढूंढिए

A  B  C  D  E  F  G  H  I  J  K  L
CAPTCHA Reality

- **Wanted:** Prevent automated access to services
- **Assumption:** Making users solve CAPTCHAS prevents automated abuse
- **Found:** Attackers uses *humans* to solve CAPTCHAS
  - Rest of abuse workflow remains automated
CAPTCHA Insight

- Are CAPTCHAs broken?
- No? CAPTCHA is hard to solve in the fully general case
  - But a *concrete family* can be solved automatically
  - Easy for CAPTCHA producer to modify family and break solver
  - Automated solvers “waste of time” (according to one service operator)
- Yes? Do *not* prevent automated abuse!
  - CAPTCHAs solved by human labor for automated tools
Insight: CAPTCHAs introduce additional cost to attacker
- $\frac{1}{10}$ cent to bypass a CAPTCHA

Insight: Deters rational profit-motivated attacker when
(cost of solving captcha) > (expected revenue)

Eliminates nuisance attacks
- Attacker business model must support added cost