CAPTCHA

EJ Jung
CAPTCHA

- stands for Completely Automated Public Turing test to tell Computers and Humans Apart
- Reverse Turing test
  - Turing test: how to tell an intelligent computer apart
  - from Wikipedia
    - it proceeds as follows: a human judge engages in a natural language conversation with one human and one machine, each of which try to appear human; if the judge cannot reliably tell which is which, then the machine is said to pass the test.
  - remember Blade Runner?
- Human Interactive Proof
Turing test example

- Imagine that two players are playing Jeopardy over the Internet by typing in answers.
- In one window, a real human person answers.
- In the other, Watson answers.
- Would you be able to tell which is which?
Robots can do more and faster

- Botnets can do even more
- Crawlers may ignore robot.txt
- Bots leave malicious contents as comments, postings, emails and collect informations
- Web spam is legal (spam is not)
  - http://www.usfca.edu/its/about/policies/aup/
Motivation for attack

➢ Search engine
  • more links, higher ranking
  • e.g. Google’s page rank

➢ Advertisement
  • mimic “word of mouth”

➢ Phishing
  • disguise as suggestions and recommendations
Motivation Beyond the Web

➢ Prevent dictionary attacks in any password system (Pinkas & Sander)
  • after failures, ask for CAPTCHA and the password

➢ Deter massive attacks
  • botnets may not pass CAPTCHA
  • humans are much slower
  • ask for CAPTCHA for any suspicious activity
Unpublished manuscript by Moni Naor first mentions automated Turing test in 1997, but not proposed or formalized.

Alta Vista patent in 1998 first practical example of using slightly distorted images of text to deter bots.

- broken later by OCR
Definition

- In 2000, formalized by Luis von Ahn, Manuel Blum & Nicholas J. Hopper of Carnegie Mellon; John Langford of IBM
- “A CAPTCHA is a cryptographic protocol whose underlying hardness assumption is based on an AI problem.”
- www.captcha.net
- Advancing AI and security together
  • battle of breaking and improving
General Approaches

- Text (ASCII/Unicode)
- Image
- Speech
- Animation
- 3-D
- Combinations of all above
Change text to look-alike: SPAM is $P4M. Fools simplest text matching.

Accented or non-English chars: Spám

Chars to words: uce@ftc.gov --> uce at ftc dot gov

URL/HTML entities: COPY becomes &cent;&#48;&Rho;&yen; or %430P%59

Better than nothing, but easy to crack

This is not technically CAPTCHA
Text Based CAPTCHAs

- **Gimpy, ez-gimpy**
  - Pick a word or words from a small dictionary
  - Distort them and add noise and background

- **Gimpy-r**
  - Pick random letters
  - Distort them, add noise and background

- **Simard’s HIP**
  - Pick random letters and numbers
  - Distort them and add arcs
Text Based CAPTCHAs
Gimpy

- First generation
  - Pick a word from dictionary
  - Random placement, font, distortion, background pattern
  - Overlapping words serve as noise.

- Frequently cracked and improved.

- In current version, 5 pairs of overlapped words. User identifies 3 words.
EZ-Gimpy

- Pick a word or words from a small dictionary
- Distort them and add noise and background

- 99% success in breaking
  - Distortion Estimation Techniques in Solving Visual CAPTCHAs, CVRP 2004
Gimpy-r

- Pick random letters
- Distort them, add noise and background

78% success in breaking Gimpy-r
- Distortion Estimation Techniques in Solving Visual CAPTCHAs, CVRP 2004
Bongo

- Visual pattern recognition puzzle
- Example: thick vs. thin
- User is presented with a new block and needs to pick left or right
Image recognition with keywords

Procedure

- display four images with the same keyword
- provide a random set of keywords to choose from
- user needs to pick the common keyword
Choose a word that relates to all the images.

TIP: You can type the first letter of a word and then use the down arrow to find it.

Submit

© 2004 Carnegie Mellon University, all rights reserved.
Beating CAPTCHA

OCR-base attacks
- http://sam.zoy.org/pwntcha/
- Pretend We’re Not a Turing Computer but a Human Antagonist

Heuristics
- vary position, warp, noise, background, colors, overlap, randomness, font, angles, language,

Accessibility problem for vision-impaired users
- audio as well as visual
- http://www.w3.org/TR/turingtest/
Classification-based approach

- **Text-based CAPTCHA Strengths and Weaknesses** [Bursztein, Martin, Mitchell CCS2011]
- Classify the given image to one of the words in synthetic corpus

**Figure 5: Example of the Blizzard pipeline**

**Figure 10: Example of the Slashdot pipeline**
Real-World Captchas Summary

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Recall</th>
<th>Precision</th>
<th>Anti-segmentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorize</td>
<td>84%</td>
<td>66%</td>
<td>background confusion</td>
</tr>
<tr>
<td>Baidu</td>
<td>98%</td>
<td>5%</td>
<td>collapsing</td>
</tr>
<tr>
<td>Blizzard</td>
<td>75%</td>
<td>70%</td>
<td>background confusion</td>
</tr>
<tr>
<td>Captcha.net</td>
<td>96%</td>
<td>73%</td>
<td>background confusion</td>
</tr>
<tr>
<td>CNN</td>
<td>50%</td>
<td>16%</td>
<td>line</td>
</tr>
<tr>
<td>Digg</td>
<td>86%</td>
<td>20%</td>
<td>line</td>
</tr>
<tr>
<td>eBay</td>
<td>95%</td>
<td>43%</td>
<td>collapsing</td>
</tr>
<tr>
<td>Google</td>
<td>0%</td>
<td>0%</td>
<td>collapsing</td>
</tr>
<tr>
<td>Megaupload</td>
<td>n/a</td>
<td>93%</td>
<td>collapsing</td>
</tr>
<tr>
<td>NIH</td>
<td>87%</td>
<td>72%</td>
<td>background confusion</td>
</tr>
<tr>
<td>Recaptcha</td>
<td>0%</td>
<td>0%</td>
<td>collapsing</td>
</tr>
<tr>
<td>Reddit</td>
<td>71%</td>
<td>42%</td>
<td>background confusion</td>
</tr>
<tr>
<td>Skyrock</td>
<td>30%</td>
<td>2%</td>
<td>background confusion</td>
</tr>
<tr>
<td>Slashdot</td>
<td>52%</td>
<td>35%</td>
<td>lines</td>
</tr>
<tr>
<td>Wikipedia</td>
<td>57%</td>
<td>25%</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Table 2: Real world captchas summary
Speech CAPTCHA

- Spell in synthesized or recorded voices
- Voice recognition vs. user’s miss rate
- Use with visual CAPTCHA for increased accessibility
  - may help attackers guess correctly
Animated CAPTCHA

- Can use Flash, MPEG, animated GIF
- Often combined with speech
- Weaknesses of Image CAPTCHA apply
- Usually *easier* to crack due to extra data for pattern matching to analyze
- Much higher processor and traffic load
- Not practical in most cases
- tEABAG_3D
- Renders the password in 3D image
- More difficult to crack than 2D images
- More resources on server
  - high load graphic processing
- Can be combined with other methods
Beating CAPTCHA by humans

- **Man-in-the-middle**
  - copy CAPTCHA from the target
  - post on the attacker’s website
  - forward the answer to the target

- **CAPTCHA factory**
  - [http://taint.org/2008/03/05/122732a.html](http://taint.org/2008/03/05/122732a.html)

- **Reuse the session id**
  - [http://www.puremango.co.uk/cm_breaking_captcha_115.php](http://www.puremango.co.uk/cm_breaking_captcha_115.php)
Adopt CAPTCHA for yourself?

➢ Free software

  • http://www.google.com/recaptcha
  • http://captcha.net
Forging Handwriting

[Ballard, Monrose, Lopresti]

Generated by computer algorithm trained on handwriting samples
Cloning a Finger

Making an Artificial Finger from a Residual Fingerprint

Materials

A photosensitive coated Printed Circuit Board (PCB)
“10K” by Sanhayato Co., Ltd.

Solid gelatin sheet
“GELATINE LEAF ”
by MARUHA CORP

320JPY/sheet

200JPY/30grams

Yokohama Nat. Univ. Matsumoto Laboratory
Cloning Process

Residual Fingerprint
- Enhancing
- Capturing
- Image Processing

Fingerprint Image
- Printing
- Mask
- Exposing
- Developing
- Etching
- Mold

Cyanoacrylate Adhesive
Adobe Photoshop 6.0

Digital Microscope
- KEYENCE VH6300: 900k pixels

Inkjet Printer
- Canon BJ-F800: 1200x600dpi
Fingerprint Image

An Enhanced Fingerprint

A Fingerprint Image

A Mask with Fingerprint Images

[Matsumoto]
Gelatin Liquid

Drip the liquid onto the mold.

Put this mold into a refrigerator to cool, and then peel carefully.
The Mold and the Gummy Finger

Mold: 70JPY/piece
(Ten molds can be obtained in the PCB.)

Gummy Finger: 50JPY/piece
Side By Side

Pores can be observed.

Enhanced Fingerprint

- Captured Fingerprint Image of the Gummy Finger with the device H (a capacitive sensor)
Play-Doh Fingers

- Alternative to gelatin
- Play-Doh fingers fool 90% of fingerprint scanners
  - Clarkson University study
- Suggested perspiration measurement to test “liveness” of the finger

[Schuckers]