Natural Interaction for Bot Detection

Original authors: Robert St. Amant and David L. Roberts

October 19, 2017

Overall

Bot detection: determining whether the user is human or computer program.

- Two traditional categories of bot detection methods
  - Human interactive proofs (HIPs): CAPTCHA
  - Human observational proofs (HOPs): input analysis
- Novel approach to bot detection
  - Human subtlety proofs (HSPs)

Overall

Motivation

Bot detection is very useful.

- Some bots are employed to register for free email accounts, which are used to send spam.
- Some bots, or so-called ‘plug-ins’, are used in massively multiuser online games (MMOGs) to gain an edge over human players, which violates the fairness and balance of the game.
- Plugins for ticket-buying, scripts for course-selection ...

Human Interactive Proofs

CAPTCHAs

CAPTHA require the user to type the letters in a specially processed image.

Human Interactive Proofs

CAPTCHAs

CAPTHA require the user to type the letters in a specially processed image.

Figure: CAPTCHA samples

Human Interactive Proofs

CAPTCHAs

CAPTHA require the user to type the letters in a specially processed image.

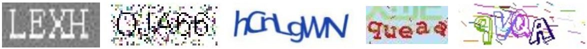

Figure: CAPTCHA samples

Sometimes, CAPTHAs are too easy for both humans and bots to recognize. However, if the difficulty is raised intending to distinguish humans from bots, it may lower user experience.

Human Interactive Proofs

Attacks to CAPTCHAs

- OCR

Human Interactive Proofs

Attacks to CAPTCHAs

- OCR
- Machine-learning-based attacks

Human Interactive Proofs

Attacks to CAPTCHAs

- OCR
- Machine-learning-based attacks
- Cheap human labor

Human Interactive Proofs

Attacks to CAPTCHAs

- OCR
- Machine-learning-based attacks
- Cheap human labor
  - $1000 per million CAPTCHAs, 2005

Human Interactive Proofs

Attacks to CAPTCHAs

- OCR
- Machine-learning-based attacks
- Cheap human labor
  - $1000 per million CAPTCHAs, 2005
  - RMB 6000 per million CAPTHCAs, 2017

Human Interactive Proofs

Attacks to CAPTCHAs

- OCR
- Machine-learning-based attacks
- Cheap human labor
  - $1000 per million CAPTCHAs, 2005
  - RMB 6000 per million CAPTHCAs, 2017
- Re-posting CAPTCHAs, unwitting human labor

Human Interactive Proofs

Variants of CAPTHA

- Speech with noise
- Image identification
- Mathematical problem solving

Human Interactive Proofs

Variants of CAPTHA

- Speech with noise
- Image identification
- Mathematical problem solving

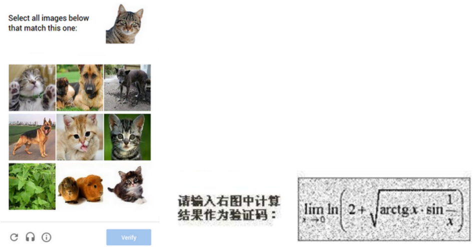
Select all images below that match this one:
Verify
请输入右图中计算结果作为验证码：
$\lim_{x\to 0}\ln\left(2+\sqrt{\operatorname{arctg}x\cdot\sin\frac{1}{x}}\right)$

Figure: Variants of CAPTCHAs

Human Observational Proofs

Method & Attack

Human observational proofs are transparent to users. They will not feel the existence of bot detection.

- Key stroke and mouse movement analysis
  - Example: anti-cheating systems in online games

Human Observational Proofs

Method & Attack

Human observational proofs are transparent to users. They will not feel the existence of bot detection.

- Key stroke and mouse movement analysis
  - Example: anti-cheating systems in online games

Attack:

- Imitation attacks:
  - scripted actions
  - pre-recorded macros

Human Subtlety Proofs

Methods

Human subtlety proofs affect users' operations slightly.

- randomly ignore user's input (mouse clicks, key strokes, etc)

Human Subtlety Proofs

Methods

Human subtlety proofs affect users' operations slightly.

- randomly ignore user's input (mouse clicks, key strokes, etc)
- randomly change the user interface (size, position of UI objects)

Human Subtlety Proofs

Methods

Human subtlety proofs affect users' operations slightly.

- randomly ignore user's input (mouse clicks, key strokes, etc)
- randomly change the user interface (size, position of UI objects)

Human Subtlety Proofs

Methods

Human subtlety proofs affect users' operations slightly.

- randomly ignore user's input (mouse clicks, key strokes, etc)
- randomly change the user interface (size, position of UI objects)

Example:

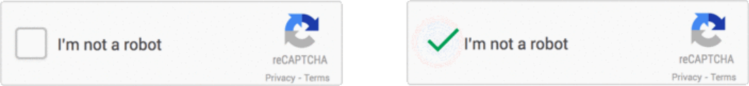

Figure: Google's No CAPTCHA ReCAPTCHA

Human Subtlety Proofs

Principles

Users will react to errors in some ways, which can be identified.

1. gaze fixation → tap → pause (to verify)
2. gaze fixation → tap → return to missed targets
3. use peripheral vision to locate targets
4. plan → tap

Human Subtlety Proofs

Principles

Users will react to errors in some ways, which can be identified.

1. gaze fixation → tap → pause (to verify)
2. gaze fixation → tap → return to missed targets
3. use peripheral vision to locate targets
4. plan → tap

Users are sensitive to the difference in error rates.

Human Subtlety Proofs

Principles

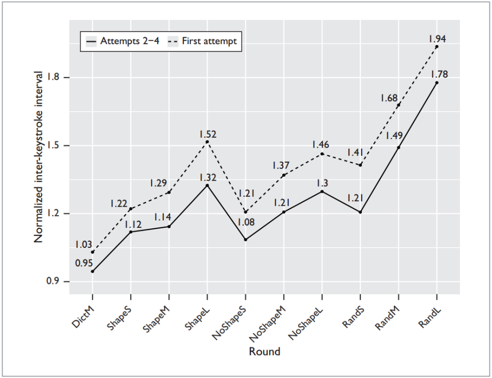

Figure: mean inter-keystroke interval for different word types

Conclusions

Comparison

	HIPs	HSPs	HOPs
Type	active	active	passive
Accuracy	high	medium	low
User Experience	bad	medium	good
Implementation	easy	hard	medium

Table: Comparison of HIPs, HSPs, HOPs

Conclusions

- HSPs combine the stengths of HIPs and HSPs, having a high accuracy with little impact to user experience.
- HSPs can be designed to be natural.
- HSPs can not only distinguish humans from bots, but also determine the type of users.
- However, HSPs sometimes mistakenly identify human users as bots, usually because of their special customs.

References

[1] Amant, Robert St., and D. L. Roberts. Natural Interaction for Bot Detection. *IEEE Internet Computing*, 20.4(2016):69-73.

[2] Hindle, Abram, M. W. Godfrey, and R. C. Holt. Reverse Engineering CAPTCHAs. *Reverse Engineering, 2008. Wcre '08. Working Conference on IEEE*, 2008:59-68.

[3] Motoyama M., Levchenko K., Kanich C., Mccoy D., Voelker G. M., and Savage S. Re: CAPTCHAs-Understanding CAPTCHA-Solving Services in an Economic Context. *Usenix Security Symposium, Washington, Dc, Usa, August 11-13, 2010, Proceedings DBLP*, 2010:435-462.

[4] Von A. L., Maurer B., Mcmillen C., Abraham D., and Blum M. "reCAPTCHA: human-based character recognition via Web security measures." *Science*, 321.5895(2008):1465.

Q & A