Baffling the Bots

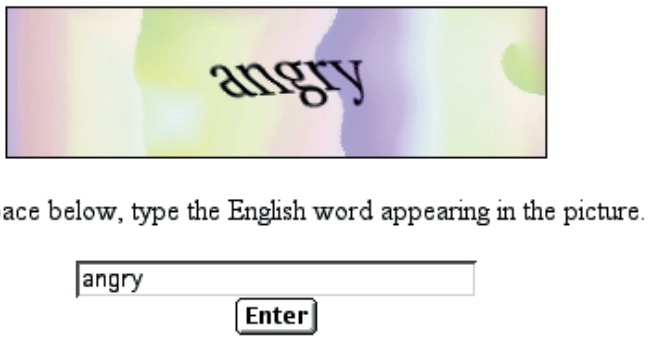
Anti-spammers take on automatons posing as humans

By LEE BRUNO

Three years ago rogue computer software programs called bots posed as teenagers in Yahoo's chat rooms on the Web. There they created mischief by collecting personal information about the teens who visited or by pointing chat participants to advertisements. The bots operated by waiting until a visitor typed a question mark. They would then automatically create a response about where a person could find an answer and provide a URL that would deliver the visitor to an advertising site.

Bots are well known for helping to generate millions of spam messages advertising printer cartridges, septic systems, Viagra and Nigerian money scams. They disseminate junk information by opening up new e-mail accounts and then automatically delivering a flood of messages. During 2001 estimates of the volume of spam reached more than six times that of a year earlier. And last year the volume was 21 times greater than in 2000, according to the Coalition against Unsolicited Bulk Email, an Australia-based organization.

E-mail filters are still rudimentary cures and pretty ineffective in curtailing the deluge of unwanted messages. After the bot incursion, Yahoo's technical staff realized that it needed to create a software gatekeeper that would allow human users in and keep automatons out. Udi Manber, Yahoo's chief scientist, went looking for help. He offered a challenge to Manuel Blum and his graduate students at the School of Computer Science at Carnegie Mellon University. Blum had an interest in investigating whether image-degradation models, which distort some part of a word or image, could be used to build a computer Turing test (named after the brilliant mathematician and a founding figure of computing Alan Turing). In 1950 Turing proposed a behavioral approach to determine whether a system could "think": a machine would pass the test if human interrogators could not tell whether replies to a series of typed questions they were asking were coming from a computer or a human.



READ THIS: A type of CAPTCHA, or image-degradation model, known as EZ-Gimpy tries to outwit computer bots with distorted letters and busy backgrounds. A human user easily recognizes the word and types it in the blank, allowing entry to a Web area.

In the course of his research, Blum came into contact with Henry Baird, a renowned figure in the computer-vision field. Baird had become familiar with the limits of computer vision from his years of work on building and analyzing systems at Lucent Technologies's Bell Labs, where he developed new software algorithms for document imaging. In 1998 he left the quiet Murray Hill, N.J., campus of Bell Labs to join another fabled institution: Xerox PARC in Palo Alto, Calif. There the armies of smart Internet bots roaming the Web to harvest information became an intellectual obsession for him.

During the fall of 2000 Baird conducted a trial at the University of California at Berkeley. The resulting paper dealt with a new image-degradation model named Pessimal Print. Concurrently, Yahoo and Blum and his team at Carnegie Mellon were working on a similar model, one version of which is called EZ-Gimpy. It is a kind of reverse Turing test, which has come to be known as a CAPTCHA, or "completely automated public Turing test to tell computers and humans apart."

CARNEGIE MELLON UNIVERSITY

These Turing tests for Internet bots are a cognitive puzzle that can be solved by humans but not by computers. "Humans are very good at reading very strange stuff," says Baird, whose formal title is principal scientist and area manager of statistical pattern and image analysis at PARC (no longer Xerox PARC).

As an example, EZ-Gimpy selects a word from an 850-word dictionary and then disfigures the letters by warping the font or leaving gaps in the letters and placing them on a busy background. In doing so, the CAPTCHA presents a human verification test to the person trying to obtain a free e-mail account or entrance to a chat room. EZ-Gimpy quickly went to work at Yahoo. And other Internet mail services, such as Microsoft's Hotmail, also use CAPTCHAs, based on EZ-Gimpy.

BAFFLETEXT: This latest generation of CAPTCHA, designed to fool particularly clever bots, employs nonsense words and type-obscuring tricks.

EZ-Gimpy has worked well, but next-generation bots are getting wise to it. They are getting better at recognizing the distorted words contained in the dictionary. But Baird, along with Monica Chew of Berkeley, co-developed BaffleText, a new CAPTCHA scheme that goes beyond the 850-word dictionary of EZ-Gimpy. It randomly generates a few degraded words each time a person logs onto a Web site to establish an e-mail account or other service. The person has to recognize the word and type it into the blank space on the page in order to progress to the next stage.

Two principal ideas guided the researchers in their quest to create a stronger deterrent for bots. BaffleText incorporates nonsense words to overcome the problem of a small dictionary. Also, it leverages Gestalt psychology, or a human's innate ability to infer the whole picture of an image from only partial information (something machines can't do). For example, BaffleText uses non-English character strings like "inchem" and "scotter" to defend against dictionary-driven attacks. What's more, its Gestalt-inspired images of words masked or degraded in appearance make it nearly impossible for a bot to decipher. Simply put, to crack BaffleText, bot programmers must solve perplexing computer-vision and pattern-recognition problems that have eluded them for decades.

To test the CAPTCHAs, other researchers from Berkeley and Carnegie Mellon are laboring to break them. And whereas the bulk of work done to date has taken place on text-based CAPTCHAs, research is under way on developing auditory and visual CAPTCHAs. All the while, the artificial-intelligence community views the challenge of trying to break CAPTCHAs as a kind of mind sport.

Baird continues to build, test and crack bots. "This is our arms race," he says. "There's no question that bots are going to become more and more sophisticated." CAPTCHAs are expected to become important to businesses in protecting their networks from smart bot intruders. In effect, they have become new electronic guardians for Web services, helping to immunize and prevent attacks from increasingly smarter bots written by people intent on abusing the services for their own gain. Meanwhile programmers are expected to unleash fleets of bots bent on breaking CAPTCHAs, thus promulgating a game of one-upmanship. That is why, for the artificial-intelligence community, building ever more powerful CAPTCHAs has provoked the same excitement once elicited by the creation of ever more sophisticated chess programs. And this work should ultimately yield a more cogent answer to the question of whether it is a human or a machine knocking at the virtual door. SA

Lee Bruno is an editor at Red Herring, *an online magazine that covers business and technology.*

HENRY S. BAIRD *PARC*