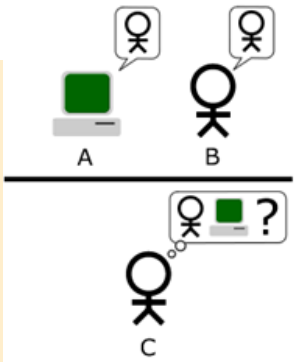
F5 Friday: An On-Demand Turing Test

Lori MacVittie, 2010-16-07

Detecting bots requires more than a simple USER_AGENT check today…

Anyone who's taken an artificial intelligence class in college or grad school knows all about the Turing Test. If you aren't familiar with the concept, it was a "test proposed by Alan Turing in his 1950 paper Computing Machinery and Intelligence, which opens with the words: "I propose to consider the question, 'Can machines think?'" Traditional Turing Tests always involve three players, and the goal is to fool a human interviewer such that the interviewer cannot determine which of the two players is human and which is a computer. There are variations on this theme, but they are almost always focused on "fooling" an interviewer regarding some aspect of the machine that it is attempting to imitate.



> Common understanding has it that the purpose of the Turing Test is not specifically to determine whether a computer is able to fool an interrogator into believing that it is a human, but rather whether a computer could imitate a human.[44] While there is some dispute whether this interpretation was intended by Turing — Sterrett believes that it was[43] and thus conflates the second version with this one, while others, such as Traiger, do not[41] — this has nevertheless led to what can be viewed as the "standard interpretation." In this version, player A is a computer and player B a person of either gender. The role of the interrogator is not to determine which is male and which is female, but which is a computer and which is a human.[45]
>
> -- Wikipedia, Turing Test

Over the past decade, as the web has grown more connected and intelligent, so too have the bots that crawl its voluminous pages attempting to index the web and make it possible for search engines like Google and Bing to be useful. Simultaneously have come the evil bots, the scripts, the automated attempts at exploiting vulnerabilities and finding holes in software that enable malicious miscreants to access data and systems to which they are not authorized. While a web application firewall and secure software development lifecycle practices can detect an attempted exploit, neither are necessarily very good at determining whether the request is coming from a bot (machine) or a real user.

Given the very real threat posed by bots, it's becoming increasingly important for organizations to detect and prevent these automated digital rodents from having access to web applications, especially business-critical applications. The trick is, however, to determine which requests are coming from bots and which ones are coming from real users. It's a trick not only because this determination is difficult to make with a high degree of confidence in the result, but because it needs to be determined *on-demand, in real-time.*

What organizations need is a sort of "on-demand Turing test" that can sort out the bots from the not bots.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com