MD5 flaw pops up in Australian traffic court

Tech Culture

August 11, 2005
11:49 PM PDT

by Declan McCullagh
@declanm

Suspected flaws in a computer algorithm have invalidated a fine issued by a speed camera in Australia.

It turns out that a Sydney magistrate **tossed out** a speeding ticket after the Roads and Traffic Authority, a government agency, failed to prove in court that the algorithm was cryptographically sound.

In other words, the argument goes, the photos could have been altered along the way. "The integrity of all speed-camera offences has been thrown into serious doubt and it appears that the RTA is unable to prove any contested speed camera matter because of a lack of admissible evidence," one defense lawyer **boasted**.

The algorithm in question, called MD5, is one of the standard choices that programmers use when creating digital signatures. But some research has suggested attacks on MD5 (though those attacks remain largely impractical).

The MD5 algorithm is known to computer scientists as a hash function. It takes any kind of input, such as a digital photograph of a car on a highway, and generates what's supposed to be a unique fingerprint. Changing even one pixel in the input file is supposed to result in a completely different fingerprint.

It's not clear what happens next. Australia's RTA could switch to a more secure algorithm (SHA-1 would be a contender) to digitally sign photographs -- or simply mount a more aggressive defense of its technique the next time this comes up in traffic court.

Tags: Tech Culture, Security