
MD5 and Speed Cameras

Tony Morris <http://tmorris.net/>

Copyright © 2006 Tony Morris

Abstract

There has been some recent controversy regarding speed camera photos and the use of the term MD5 seems to have been taken well out of context as a result. MD5 is what is known as a hash algorithm or one way function. It is sometimes erroneously referred to as an encryption algorithm or cipher - this is simply false. Some other absurd claims are that "MD5 is susceptible to viruses" or that "MD5 ensures cryptographic security". These statements are to be ignored as nothing more than typical media hype.

What is MD5?

MD5 is called a hash algorithm or one way function because once computed, there is no mathematically feasible way to derive the original input from the result. To draw an analogy to a function that is not one way, consider taking the number 3 (the input), multiplying it by 5 (the function) and obtaining 15 (the result). If I were to ask you to derive the input from the result, you could do it quite easily simply by reversing the function; that is, instead of multiplying by 5, you would divide by 5. Thus, 15 divided by 5 is 3, and so you have the original input. This can not be achieved with a one way function and it is this property that gives one way functions a unique application.

If I were to hand you a document (the input), calculate the MD5 of it (the function) and hand you the result, there is no way to derive the input document from that result, therefore, this is a form of ensuring integrity of that document. That is to say, if I handed you a document, and the MD5 hash result, you could be certain (within some specific bounds) that the original document has not been modified during its transit to you. You could ensure this by calculating the MD5 hash yourself and checking that it matches the one you were given. If it matches, the document has not been tampered with since its original MD5 hash was calculated.

MD5, and all known hash algorithms, use a special type of security to make the guarantee that they are genuine one way functions (that there is no flaw in the algorithm that makes it easy to reverse). This security is proven to be breakable, which might be contrary to the messages that you will be receiving from your road traffic authority in the future. That is, all known hash algorithms are breakable and this can be proven. So why use them? Most hash algorithms cannot exploit this fact because it is computationally impractical. That is to say, the required computing power to exploit this vulnerability exceeds the amount of conventional computing power that we have today. It is important to note here that the computing power of some intelligence agencies, such as the National Security Agency (USA) and Defence Signals Directorate (Australia) should not be considered 'conventional', and therefore, no guarantees can be made here - historical observations of national intelligence plausibly arouse speculation among conspiracy theorists.

MD5 and Speed Cameras

Speed camera photographs are typically associated with an MD5 hash in a flawed attempt to verify integrity of the photograph. That is to say, in transit from the camera to your letter box, integrity of the document can be (but isn't) guaranteed, since any modifications of the document would mean that a different MD5 hash is generated upon verification. First and foremost, MD5 is a weak hash algorithm, and does not even ensure document integrity in a practical sense, since it can be demonstrated to be broken. Second, any hash algorithm is mathematically proven to be breakable, which may be considered insufficient by a court.

Finally, and perhaps most amusingly, the photograph and associated hash are not digitally signed. I'm sure that anyone who has any knowledge of electronic security would find this oversight somewhat

astonishing, but it must be highlighted that we are dealing with the traffic authorities in the land down under, where surprises are really just expectations. Digital signing is a way of ensuring that the entire document and hash were not modified during transit assuming that the cryptographic key is kept safe.

Consider the analogy; a document is written down on paper and signed. A special property of that paper is that any modification of its contents means that the signature dissolves. Therefore, if I handed you a signed document, you could be certain that whoever signed that document, signed it with the exact same contents that you are now observing, thus providing some form of integrity. However, you cannot be sure "who" signed the document, and you also cannot be assured against the possibility that the original document may have been thrown away, and a new fraudulent copy was substituted along with some other hash during transit. It is this trivial oversight on the part of the traffic authorities that digital signing is designed to solve.

A digital signature would require that each speed camera possess a unique private key that it kept secret. Any leak of that private key would render the entire authentication and integrity checking system useless, however, no more or less useless than it already is. This system is often referred to as public key cryptography or Public Key Infrastructure (PKI) and is integrated into most web browsers to ensure secure communication between your web browser and the destination web server. It is designed in such a way that given a digitally signed document, only the holder of the private key that signed it could have produced that document, in this case, the camera that took the photograph. The private key is not a required artefact to perform integrity checking should the need arise, therefore, it can remain a secret to the camera.

Some recent court cases against speed camera notices include lawyer Dennis Miralis, who successfully defended a case by requesting that the prosecution (RTA) prove that the picture could not have been altered, even though it has an associated MD5 hash. The RTA could not produce an expert witness to testify. Although it is quite clear from some of the comments of both the defense and prosecution that neither really understand what a hash algorithm is, it is absurd to suggest that a hash algorithm does make this guarantee, since it is well established that hash algorithms are all known to be theoretically breakable. It would be interesting to hear what an expert witness would have said had one been sought by the prosecution.

Another case, again defended by Dennis Miralis, exploited the fact that the Road Traffic Act section 47 (2) (c), which deals with "security indicators" says that a speed camera photograph code must be comprised of "letters, numbers and symbols". All MD5 hash results are 128-bits (or 16 bytes), which when viewed with a hexadecimal viewer, are comprised only of numbers and letters (0-9 and A-F), but not symbols, and the absence of symbols does not meet the criteria for "security codes". The Act has since been amended to read "letters, numbers or symbols". In any case, this clearly demonstrates the ignorance of those who create the legislation, and also of those who test it. If it's not obvious, a hexadecimal representation is just that, a representation. An MD5 hash result is a sequence of 128 bits; how they are represented is entirely superficial, since there are an infinite possible number of representations. For example, one might represent an MD5 hash using a binary representation, where only 0 or 1 are used, or an octal representation, where only 0-7 are used. Therefore, an MD5 hash is no more "letters, numbers or symbols" than it is heiroglyphics, braille, a set of switched christmas tree lights or any arbitrary data representation.

Conclusion

Our road traffic authorities have made many bungles in the past, and trends suggest that they will continue to make them in the future. The emphasis on the enforcement of speed limits has been shown to contribute to increased danger and a rise in fatalities on public roads in independent reports. A significant upgrade of speed measuring equipment and legislation is required before this type of law enforcement can even be considered in any way authentic. If you have received an infringement notice as a result of a speed camera related offence, please do some research and challenge it in court. I do not condone excessive speed if it ultimately endangers lives, however, I am a fervent supporter of increasing road safety, which means that traffic authorities are a declared enemy whose sole intent is arguably, to make profits at the expense of lives. War knows of no ethic; we must fight with whatever weapon is at our disposal.

About the Author

Popular requests for a statement of authority have finally seen me concede. I completed my bachelor degree (Information Technology) in 2001 and up until February 2006, I have worked for IBM Australia as a Software Engineer developing software for the IBM Tivoli security brand. I work on a component called GSKit (Global Security Kit), which is the security software that is used by all IBM products such as IBM WebSphere Application Server and IBM Java Development Kit. The software provides, among many things, the function of many popular cryptographic and hash algorithms that are used heavily in security software production. Some of our clients include General Motors, National Australia Bank and Westpac Bank.

I don't consider myself a security "guru" (unlike a few of those that work next to me) despite any claims to the contrary by others, while at the same time, I don't think MD5 or any hash algorithm requires a "guru" to fully understand - it is really quite trivial in the greater scheme of digital security. In the event that more credibility is sought, my CV can be viewed at <http://tmorris.net/cv/>.

References

RFC 1321 The MD5 Message-Digest Algorithm
<http://www.ietf.org/rfc/rfc1321.txt>

How to Break MD5 and Other Hash Functions
<http://www.infosec.sdu.edu.cn/paper/md5-attack.pdf>

Public Key Infrastructure
http://en.wikipedia.org/wiki/Public_key_infrastructure

RoadSense - a Commonsense Road Safety Initiative
<http://www.roadsense.com.au/>