# MD5 and Perspectives

## last updated 1-1-2009

A group of researchers recently announced an attack that subverts the public key infrastructure (PKI) used by web browsers to authenticate servers when using HTTPS. As described in the paper the researchers exploit MD5 collisions to create a rogue Certificate Authority (CA) certificate capable of create malicious server certificates that are trusted by all major browsers.
We have received a good number of questions about how this announcement affects Perspectives. As described below, Perspectives can help users detect malicious certificates such as those generated by the rogue CA. Additionally, we describe why the attack used in this work does not undermine the security of Perspectives, even though Perspectives uses MD5.

## Attack Overview: Using MD5 Collisions to Create a Rogue CA

Please read their paper for details, this is just a high-level overview.

As noted by the authors, their attack uses an MD5 weakness has been well-known for some time. The main contribution of their work is crafting a real-world attack by leveraging the poor security practices of some CAs.

To understand the implications (and limitations) of the MD5 vulnerability, it necessary to distinguish between two properties of cryptographic hash functions:

1. **Collision Resistance:** A hash function H is collision resistant if it is hard to find two different messages m1 and m2 such that H(m1) == H(m2)
2. **Second Preimage Resistance** A hash function H is second preimage resistant if given a message m1, it is hard to find a second message m2 different from m1 such that H(m1) == H(m2)

The difference is subtle but important: it is much easier to break collision resistance than it is to break second preimage resistance, a collision resistance attacker has the flexibility to choose both m1 and m2 in a way that makes finding a collision easier. *For MD5 collision resistance is known to be broken, but second-preimage resistance is not.* The rogue CA attack uses a weakness in MD5 collision resistance to undermine the

traditional CA trust model used by browsers. As described below, Perspectives requires only second preimage resistance of MD5.

The published attack creates a rogue CA certificate using an MD5 collision. In terms of the above definition, the researchers create a file m1 that is a certificate request for a domain name the researchers legitimately own. They then pay a real CA that is trusted by all browsers to grant a certificate for m1. The attack arises from the fact that the researchers were also able to create a file m2 that is a malicious certificate request claiming that the researchers are themselves a trusted CA. While a legitimate CA would never generate a certificate saying that the researchers are a CA, the researchers can actually generate the certificate themselves using the signature of the valid certificate (created from m1). Why does this work? Well, when a CA creates the signature in a certificate, for efficiency, it computes the signature over the hash of the data in the certificate request. Thus, since the researchers found a collision H(m1) == H(m2), the signature in the original valid certificate will also work as a signature for the malicious certificate.

Once the researchers have a rogue CA certificate that browsers will trust as a valid CA certificate, they can use that CA certificate to grant themselves a certificate for ANY domain name. This would allow them to impersonate Google, your bank, or just about any other HTTPS website. That is scary!

## How can Perspectives help defend against this attack?

One use of Perspectives is to provide an additional layer of protection to detect attacks even when the browser trusts the CA that signed the certificate. This recent attack is a great example of why Perspectives can be useful.

Let's look at an example were a rogue CA is used maliciously to generate a certificate for www.google.com . The attacker can launch a "man-in-the-middle" attack on your web connection while you are using wireless and impersonates Google using the malicious certificate. Normally, your browser would just trust this certificate without asking any questions because it trusts the root CA. Perspectives, on the other hand, completely ignores all CA trust data and instead trusts a key based on whether a collection of network notaries (scattered throughout the Internet) have seen www.google.com using that key consistently over time. Since the notary servers will still

see www.google.com's correct certificate and report that key to the client, the client will be able to detect that the attacker's certificate is suspicious and reject it.

To allow Perspectives to detect these attacks, you must instruct it to contact Notaries for all HTTPS sites, even if your browser considers the certificate valid. To do so, use Tools -> Add-ons -> Perspectives and then click on the "Preferences" tab and select the option "Contact Notaries for all HTTPS sites".

## Perspectives's use of MD5:

Perspectives uses MD5 in two ways. However, both uses depend only on the second preimage resistance of MD5 and thus are not undermined by the published weakness in MD5 collision resistance. In more detail:

1. When a Notary server monitors the keys of a remote server, it stores this key in its database as an MD5 hash. Clients request these hash values from the server and then compare them against the hash of the key they received directly over the network. Let's look at what it would take for an attacker to use MD5 to subvert this mechanism to launch a man-in-the-middle attack on www.example.com. A notary server contacts www.example.com periodically and receives a key k1, which it stores as H(k1). At some point, a client tries to connect to www.example.com but the attacker injects a bogus key k2 as part of a man-in-the-middle attack. When checking the key against notary replies, the client will test if H(k1) == H(k2), rejecting k2 if the values do not match. As you can see, because the attacker must find a value k2 with the same hash value as the fixed k1, this is an example of second pre-image resistance as described above. Because MD5's second preimage resistance is still secure, this attack will fail.
2. Perspectives also uses MD5 as the digest algorithm for the signatures generated by notaries and used by clients to assure that they have received authentic notary data. That is, given a notary response n1, the signature is is computed using RSA-sign(H(n1)). Thus, if an attacker was able to generate a falsified notary response n2 such that H(n1) == H(n2), then the client would accept it as valid. However, this again requires breaking second preimage resistance.

Despite the fact that no efficient attacks on MD5 second preimage resistance are known to exist, the weaknesses demonstrated against MD5 collision resistance suggest that researchers are also likely to make progress on breaking MD5 second preimage resistance in the not-to-distant future. As a result, we plan on moving Perspectives to a stronger hash function like SHA-256 in the near future.

## FAQ:

**Q:** Why does Perspectives consider the certificate for the “rogue CA” example site (https://i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org/ ) cert to be valid?

**A:** Perspectives ignores all CA information in a certificate, so the MD5 attack has no impact on whether the cert is considered valid. Perspectives only cares what key the notaries see a particular domain using. Since the researchers giving the demo are the legitimate owners of https://i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org/, Perspectives will consider the certificate valid once it has built up sufficient history. As described above, if the researchers tried to claim that their website was in fact www.google.com, the notaries would detect a conflict and not trust the certificate.