

# 1400 - How we created the first SHA-1 collision and what it means for hash security

Friday at 14:00 in Track 4

45 minutes | Demo, Tool

**Elie Bursztein\***Anti-abuse research lead, Google\*

In February 2017, we announced the first SHA-1 collision. This collision combined with a clever use of the PDF format allows attackers to forge PDF pairs that have identical SHA-1 hashes and yet display different content. This attack is the result of over two years of intense research. It took 6500 CPU years and 110 GPU years of computations which is still 100,000 times faster than a brute-force attack.


In this talk, we recount how we found the first SHA-1 collision. We delve into the challenges we faced from developing a meaningful payload, to scaling the computation to that massive scale, to solving unexpected cryptanalytic challenges that occurred during this endeavor.

We discuss the aftermath of the release including the positive changes it brought and its unforeseen consequences. For example it was discovered that SVN is vulnerable to SHA-1 collision attacks only after the WebKit SVN repository was brought down by the commit of a unit-test aimed at verifying that Webkit is immune to collision attacks.

Building on the Github and Gmail examples we explain how to use counter-cryptanalysis to mitigate the risk of a collision attacks against software that has yet to move away from SHA-1. Finally we look at the next generation of hash functions and what the future of hash security holds

Elie Bursztein

Elie Bursztein leads Google's anti-abuse research, which helps protect users against Internet threats. Elie has contributed to applied-cryptography, machine learning for security, malware understanding, and web security; authoring over fifty research papers in the field. Most recently he was involved in finding the first SHA-1 collision.

Elie is a beret aficionado, tweets at @elie, and performs magic tricks in his spare time. Born in Paris, he received a Ph.D from ENS-cachan in 2008 before working at Stanford University and ultimately joining Google in 2011. He now lives with his wife in  [Mountain View, California](#).

@elie

#defcon25/by\_track/track4/Friday

#defcon25/By\_Day/\_Friday